



(19) **EP 1 085 443 A2**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:

21.03.2001 Bulletin 2001/12

(21) Application number: 02300024.9

(22) Date of filing: 14.08.2000

(84) Designated Contracting States:

AT BE CH CY DE DK ES FI FR GB GR IE IT LU

MC NL PT SE

Designated Extension States:

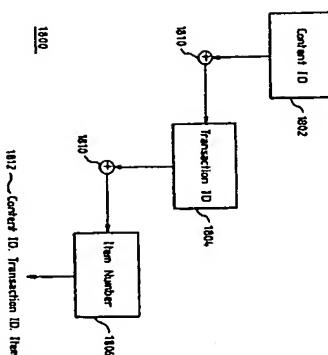
AL LT LV MR RO SI

(30) Priority: 17.08.1999 US 397419

(71) Applicant: **International Business Machines Corporation**, Armonk, N.Y. 10504 (US)

(54) **Method and apparatus for uniquely identifying a customer purchase in an electronic distribution system**

(57) A system for tracking usage of digital content for distributing digital content over a computer readable medium to users. The content sites associate unique content identifier with the content associated. Electronic stores coupled to a network sell licenses to play digital content to users. The licenses contain a unique transaction identifier for uniquely identifying the transaction, and the licenses contain a unique item identifier for uniquely identifying at least one item in the transaction. Content players, which receive from the network the licensed content data, are used to play the licensed content data. The content players produce a purchase identifier based upon the mathematical combination of the content identifier, the transaction identifier and the item identifier.



[0002] The use of global distribution systems such as the Internet for distribution of digital assets such as music, film, computer programs, pictures, games and other content continues to grow. At the same time owners and publishers of valuable digital content have been slow to embrace the use of the Internet for distribution of digital assets for several reasons. One reason is that owners are afraid of unauthorized copying or printing of digital content. The electronic delivery of digital content removes several barriers to printing. One barrier that is removed with electronic distribution is the requirement of the tangible recordable medium itself (e.g. diskettes or CD ROMs). It costs money to copy digital content on tangible media, albeit, in many cases less than a dollar for a blank tape or recordable CD. However, in the case of electronic distribution, the tangible medium is no longer needed. The cost of the tangible medium is not a factor because content is distributed electronically. A second barrier, is the format of the content itself i.e. is the content stored in an analog format versus a digital format. Content stored in an analog format, for example, a printed picture, when reproduced by photocopying, the copy is of lesser quality than the original. Each subsequent copy of a copy, sometimes called a generation, is of less quality than the original. This degradation in quality is not present when a picture is stored digitally. Each copy, and every generation of copies can be as clear and crisp as the original. The aggregate effect of perfect digital copies combined with the very low cost to distribute electronically and to distribute content widely over the Internet makes it relatively easy to pirate and distribute unauthorized copies. With a couple of keystrokes, a pirate can send hundreds or even thousands of perfect digital assets distributed electronically over the Internet. Therefore a need exists to ensure the protection and security of digital assets distributed electronically.

[0003] Providers of digital content desire to establish a secure, global distribution system for digital content that protects the rights of content owners. The problems with establishing a digital content distribution system include developing systems for digital content electronic distribution, rights management, and asset protection. Digital content that is distributed electronically includes content such as print media, film, games, programs, television, multimedia, and music.

[0004] The deployment of an electronic distribution system provides the digital content providers the ability to achieve fast settlement of payment through redistribution of content. Since the electronic digital content distribution system is not affected by physical inventory outages or returns, the digital content providers could facilitate new, or augment existing, distribution channels for better time-usage of inventory. The transaction data from the electronic distribution system could be used to obtain information regarding consumer buying patterns as well as to provide immediate feedback on electronic marketing programs and promotions. In order to meet these goals, a need exists for digital content providers to use an electronic distribution model to make digital content available to a wide range of users and businesses while ensuring protection and metering of digital assets.

[0005] Other commercially available electronic distribution systems for digital content, such as real audio, A2B from AT&T, Liquid Audio Pro from Liquid Audio Pro Corp., City Muilo Network from Audio Soft and others offer transmission of digital data over secured and unsecured electronic networks. The use of secured electronic networks greatly reduces the requirement of digital content providers of distributing content to a wide audience. The use of unsecured networks such as the Internet and Web allows the digital content to arrive to an end-user securely such as through the use of encryption. However, once the encrypted digital content is de-encrypted on the end-user's machine, the digital content is readily available to the end-user for unauthorized redistribution. Therefore a need exists for a secure digital content electronic distribution system that provides protection of digital assets and ensures that the 'Content Provider's' rights are protected even after the digital content is delivered to consumers and businesses. A need thus exists for rights management to allow for secure delivery, licensing, authorization, and control of the usage of digital assets.

[0006] Another reason owners of digital content have been slow to embrace electronic distribution is their desire to maintain and foster existing channels of distribution. Most content owners sell through retailers. In the music market Web sites that allow Internet users to make selections over the Internet and have selections mailed to the end-user. Example music Web sites include iGtowner, Music Boulevard and Columbia House. The use of electronic distribution can remove the ability of the retail sites from differentiating themselves from each other and differentiate themselves

DISCLOSURE OF THE INVENTION

[0016] It is an object of the present invention to remove the above-mentioned drawbacks and to provide a system for tracking usage of content data. One embodiment of the present invention provides a system for tracking usage of digital content on user devices. Content data for distributing digital content over a computer readable medium to users. The content data associates unique content identifier with the content associated. Electronic stores coupled to a network, identifying the transaction, and the licensee contains a unique transaction identifier for uniquely identifying at least one item in the transaction. Content players, which receive from the network the licensed content data, are used to play the licensed content data. The content players produce a purchase identifier based upon the mathematical combination of the content identifier, the transaction identifier and the item identifier.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] The invention will now be described, by way of example only, with reference to the accompanying drawings in which:

FIG. 1 is a block diagram illustrating an array of a Series Digital Content Processor, also known as

FIG. 2 is a block diagram of a system for automatically selecting a communication channel for a telephone connection.

FIG. 5 is a block diagram illustrating an overview of the layers for the Rights Management Architecture of the

FIG. 6 is a block diagram illustrating an overview of the Content Distribution and Licensing Control as it applies to

FIG. 8 is a block diagram of the major tools, components and processes of the Work Flow Manager corresponding

SCHOOL OF THE SOUL: A JOURNAL OF LITERATURE AND CULTURE

FIG. 11. Flow diagram of a method to calculate an encoding rate factor for the Content Preprocessing and

Acquisition Tool of FIG. 8:

FIG. 14 is an example of user interface screens of the Player Application demonstration contained in a local library.

FIG. 15 is a block diagram illustrating the major components and processes of a Player Application running on

FIG. 17 is a flow diagram of an alternate embodiment to automatically retrieve additional information for the ATR.

DETAILED DESCRIPTION OF THE INVENTION

sections in this amendment.

1. REQUIREMENTS

A System Overview

VII. CLEARINGHOUSE(S)

6

8

of the authenticity and integrity of the Digital Content. The advantage of these rights management functions is that the electronic Digital Content distribution infrastructure does not have to be secure or trusted. Therefore allowing transmission over network infrastructures such as the Web and Internet. This is due to the fact that the Content is encrypted within Secure Containers and its storage and distribution are separate from the control of its unlocking and use. Only users who have decryption keys can unlock the encrypted Content, and the Clearinghouse(s) releases decryption keys only for authorized and appropriate usage requests. The Clearinghouse(s) will not clear bogus requests from unknown or unauthorized parties or requests that do not comply with the content's usage conditions as set by the content provider. In addition, if the SC is tampered with during its transmission, the software in the Clearinghouse(s) determines that the Content in a SC is corrupted or falsified and repudiate the transaction.

[0025] The control of Content usage is enabled through the End-User Player Application 185 running on an End-User Device(s). The application embeds a digital code in every copy of the Content that defines the allowable number of secondary copies and play backs. Digital watermarking technology is used to generate the digital code, to keep it hidden from other End-User Player Application 185, and to make it resistant to alteration attempts. In an alternate embodiment, the digital code is just kept as part of the usage conditions associated with the Content 113. When the Digital Content 113 is downloaded in a compliant End-User Device(s), the End-User Player Application 185 reads the watermark to check the use restrictions and updates the watermark as required. If the requested use of the content does not comply with the usage conditions, e.g., the number of copies has been exhausted, the End-User Device(s) will not perform the request.

[0026] Content watermarking also provides the means to identify the origin of authorized or unauthorized copies of Content. An initial watermark in the Content is embedded by the content proprietor to identify the content proprietor, specify copyright information, define geographic distribution areas, and add other pertinent information. A second watermark is embedded in the Content at the End-User Device(s) to identify the content purchaser (or licensee) and End-User Device(s), specify the purchase or license conditions and date, and add any other pertinent information.

[0027] Since watermarking becomes an integral part of the Content, they are carried in the copies independent of whether or the copies were authorized or not. Thus the Digital Content always contains information regarding its source and its permitted use regardless of where the content resides or where it comes from. This information may be used to combat illegal use of the Content.

2. Watermarking

[0028] As part of its rights management functions, the Clearinghouse(s) keeps a record of all transactions where a key exchange is cleared through the Clearinghouse(s). This record allows for the monitoring of licensing, authorization and the original conditions of use. The transaction record can be reported to responsible parties, such as, content proprietor or Content Provider(s), retailers, and others, on an immediate or periodic basis to facilitate electronic reconciliation of transaction payments and other uses.

3. Open Architecture

[0029] The Secure Digital Content Electronic Distribution System (System) is an open architecture with published specifications and interfaces to facilitate broad implementation and acceptance of the System in the marketplace while maintaining rights protection for the content proprietors. The flexibility and openness of the System architecture also enable the System to evolve over time as various technologies, implementation infrastructures, and devices are delivered to the marketplace.

[0030] The architecture is open regarding the nature of the Content and its format. Distribution of audio, programs, multimedia, video, or other types of Content is supported by the architecture. The Content could be in a native format, such as linear PCM for digital music, or a format achieved by additional preprocessing or encoding, such as streaming, compression, or pseudo-streaming, and more. The architecture is open to various encryption and watermarking techniques. It allows for the selection of specific techniques to accommodate different Content types and formats and to the marketplace.

[0031] The architecture is also open to different distribution networks and distribution models. The architecture supports content distribution over low-speed Internet connections or high-speed satellite and cable networks and can be used with point-to-point or broadcast models. In addition, the architecture is designed so that the functions in the End-User Device(s) can be implemented on a wide variety of devices, including low cost consumer devices. This flexibility allows Content Provider(s) and retailers to offer Content to Internet or End-User(s) through a variety of service offerings and enables the users to purchase or license Content, play it back, and record it on various compliant player devices.

B. System Functional Elements

[0032] Turning now to FIG. 1, there is shown a block diagram illustrating an overview of a Secure Digital Content Electronic Distribution System 100 according to the present invention. The Secure Digital Content Electronic Distribution System 100 encompasses several business elements that comprise an end-to-end solution, including: Content Provider(s) 101 or the proprietors of the Digital Content, Electronic Digital Content Store(s) 103, Intermediate Market Partners (not shown), Clearinghouse(s) 105, Content Hosting Site 111, Transmission Infrastructure 107, and End-User Device(s) 109. Each of these business elements use various components of the Secure Digital Content Electronic Distribution System 100. A high level description of these business elements and system components, as they pertain specifically to electronic Content 113 distribution, follows.

1. Content Provider(s) 101

[0033] Content Provider(s) 101 or content proprietor(s) are owners of original Content 113 and/or distributors authorized to package independent Content 113 for further distribution. Content Provider(s) 101 may exploit their rights directly or license independent Content 113 to the Electronic Digital Content Store(s) 103, or Intermediate Market Partners (not shown), usually in return to Content usage payments related to electronic commerce revenues. Examples of Content Provider(s) 101 include Sony, Time-Warner, MTV, IBM, Microsoft, Turner, Fox and others.

[0034] Content Provider(s) 101 use tools provided as part of the Secure Digital Content Electronic Distribution System 100 in order to prepare their Content 113 and related data for distribution. A Work Flow Manager Tool 154 schedules Content 113 to be processed and tracks the Content 113 as it flows through the various steps of Content 113 preparation and packaging to maintain high quality assurance. The term media is used throughout this document to mean data related to the Content 113 and in this embodiment does not include the Content 113 itself. As an example, metadata for a song may be a song title or song credits but not the sound recording itself. It is used to extract metadata from the Content Provider(s) 101 Database 160 or data provided by the Content Provider(s) in a prescribed format (for a music example the Content 113 information such as CD title, artist name, song title, CO artwork, and more) and to package it for electronic distribution. The Metadata Administration and Entry Tool 161 is also used to enter the Usage Conditions for the Content 113.

[0035] The encrypted Content 113, digital content-related data or metadata, and encrypted keys are packed in SCE (described below) by the SCE Packer Tool and stored in a content hosting site and/or promotional web site for electronic distribution. The content hosting site can reside at the Content Provider(s) 101 or in multiple locations, including Electronic Digital Content Store(s) 103 and Intermediate Market Partners (not shown) facilities. Since both the Content 113 and the keys (described below) are encrypted and packed in SCE, Electronic Digital Content Store(s) 103 or any other hosting agent can not directly access decrypted Content 113 without clearance from the Clearinghouse(s) and notification to the Content Provider(s) 101.

2. Electronic Digital Content Store(s) 103

[0036] Electronic Digital Content Store(s) 103 are the entities who market the Content 113 through a wide variety of services or applications, such as Content 113 theme programming or electronic merchandising of Content 113. Electronic Digital Content Store(s) 103 manage the distribution, development, business operations, settlements, merchandising, and sales of their services. Examples online digital content, Content 113 theme programming or electronic merchandising, and marketing, and sales of their services.

[0037] Within their services, Electronic Digital Content Store(s) 103 implement certain functions of the Secure Digital Content Electronic Distribution System 100. Electronic Digital Content Store(s) 103 aggregate information from the Content Provider(s) 101, pack content and metadata in additional SCs, and deliver these SCs to consumers or businesses as part of a service or application. Electronic Digital Content Store(s) 103 use tools provided by the Secure Digital Content Electronic Distribution System 100 to assist with: metadata extraction, secondary usage conditions, SC packaging, and tracking of electronic content transactions. The secondary usage conditions data can include retail business offers such as Content 113 purchase price, pay-per-item price, copy authorization and target device types, or timed-availability restrictions.

[0039] Once an Electronic Digital Content Store(s) 103 completes a valid request for electronic Content 113 from an End-User(s), the Electronic Digital Content Store(s) 103 is responsible for authorizing the Clearinghouse(s) 105 to release the decryption key for the Content 113 to the customer. The Electronic Digital Content Store(s) also authorizes the download of the SC containing the Content 113 to the customer. The Electronic Digital Content Store(s) may elect to host the SCs containing the Digital Content at its local site and/or utilize the hosting and distribution facilities of another Content hosting site.

[0039] The Electronic Digital Content Store(s) can provide customer service for any questions or problems that an End-User(s) may have using the Secure Digital Content Store(s) to contact their customer service support to the Clearinghouse(s) 105. Content Store(s) 103 may contact their customer service support to the Clearinghouse(s) 105.

3. Intermediate Market Partners (not shown)

[0040] In an alternate embodiment, the Secure Digital Content Electronic Distribution System 100 can be used to provide Content 113 securely to other businesses called Intermediate Market Partners. These partners may include digital content-related companies offering a non-electronic service, such as television stations or video clubs, radio stations or record clubs, that distribute Content 113. These partners may also include other trusted parties who handle material as part of making or marketing sound recordings, such as record studios, replicators, and producers. These Intermediate Market Partners requires clearance from the Clearinghouse(s) 105 in order to decrypt the Content 113.

4. Clearinghouse(s) 105

[0041] The Clearinghouse(s) 105 provides the licensing authorization and record keeping for all transactions that relate to the sale and/or permitted use of the Content 113 encrypted in a SC. When the Clearinghouse(s) 105 receives a request for a decryption key for the Content 113 from an intermediate or End-User(s), the Clearinghouse(s) 105 validates the integrity and authenticity of the information in the request; verifies that the request was authorized by an Electronic Digital Content Store(s) or Content Provider(s) 101; and verifies that the requested usage complies with the content Usage Conditions as defined by the Content Provider(s) 101. Once these verifications are satisfied, the Clearinghouse(s) 105 sends the decryption key for the Content 113 to the requesting End-User(s) packed in a Content SC. The key is encrypted in a manner so that only the authorized user can retrieve it. If the End-User's request is not verifiable, complete, or authorized, the Clearinghouse(s) 105 rejects the request for the decryption key.

[0042] The Clearinghouse(s) 105 keeps a record of all transactions and can report them to responsible parties, such as Electronic Digital Content Store(s) 103 and Content Provider(s) 101, on an immediate, periodic, or restricted basis. This reporting is means by which Content Provider(s) 101 can be informed of the sale of Content 113 and the Electronic Digital Content Store(s) 103 can obtain an audit trail of electronic delivery to their customers. The Clearinghouse(s) 105 can also notify the Content Provider(s) 101 and/or Electronic Digital Content Store(s) 103 if it detects that information in a SC has been compromised or does not comply with the Content's Usage Conditions. The transaction recording and repository capabilities of the Clearinghouse(s) 105 database is structured for data mining and report generation.

[0043] In another embodiment, the Clearinghouse(s) 105 can provide customer support and exception processing for transactions such as refunds, transaction failure, and purchase dispute. The Clearinghouse(s) 105 can be operated as an independent entity, providing a trusted custodian or rights management and marketing. It provides Billing and settlement as required. Examples of electronic Clearinghouse(s) include Secure-e-Bank.com and Secure Electronic Transaction (SET) from Visa/Mastercard. In one embodiment, the Clearinghouse(s) 105 are Web sites accessible to the End-User Device(s) 109. In another embodiment, the Clearinghouse(s) 105 is part of the Electronic Digital Content Store(s) 103.

5. End-User Device(s) 109

[0044] The End-User Device(s) 109 can be any player device that contains an End-User Player Application 195 (described later) compliant with the Secure Digital Content Electronic Distribution System 100 specifications. These devices may include PCs, set-top boxes (STBs), and Internet appliances. The End-User Player Application 195 could be implemented in software and/or consumer electronics hardware. In addition to performing play, record, and library management functions, the End-User Player Application 195 performs SC processing to enable rights management. In the End-User Device(s) 109, the End-User Device(s) 109 manages the download and storage of the SCs containing the Digital Content requests and manages receipt of the encrypted Digital Content keys from the Clearinghouse(s) 105; processes the watermark(s) every time the Digital Content is copied or played; manages the number of copies made (or deletion of the copy); in accordance with the Digital Content Usage Conditions; and performs the copy to an external media or portable consumer device if permitted. The portable consumer device can perform a subset of

the End-User Player Application 195 functions in order to process the content's Usage Conditions embedded in the watermark. The terms End-User(s) and End-User Player Application 195 are used throughout this to mean through the use or running-on an End-User Device(s) 109.

6. Transmission Infrastructures 107

[0045] The Secure Digital Content Electronic Distribution System 100 is independent of the transmission network connecting the Electronic Digital Content Store(s) 103 and End-User Device(s) 109. It supports both point-to-point such as the Internet, and broadcast distribution models such as digital broadcast television.

[0046] (Even though the same tools and applications are used to acquire, package, and track Content 113 transactions over various Transmission Infrastructures 107, the presentation and method in which services are delivered to the customer may vary depending on the infrastructure and distribution model selected. The quality of the Content 113 being transferred may also vary since high bandwidth infrastructures can deliver high-quality digital content at more acceptable response times than lower bandwidth infrastructures. A service application designed for a point-to-point distribution model can be adapted to support a broadcast distribution model as well.

C. System Uses

[0047] The Secure Digital Content Electronic Distribution System 100 enables the secure delivery of high-quality, electronic copies of Content 113 to End-User Device(s) 109, whether consumer or business, and to acquire and track usage of the Content 113.

[0048] The Secure Digital Content Electronic Distribution System 100 could be deployed in a variety of consumer and business-to-business services using both new and existing distribution channels. Each particular service could use a different financial model that can be enforced through the rights management features of the Secure Digital Content Electronic Distribution System 100. Models such as wholesale or retail purchase, pay-per-item usage, subscription services, copy/no-copy restrictions, or redistribution could be implemented through the rights management of the Clearinghouse(s) 105 and the End-User Player Application 195 copy protection features.

[0049] The Secure Digital Content Electronic Distribution System 100 allows Electronic Digital Content Store(s) 103 and Intermediate Market Partners a great deal of flexibility in creating services that sell Content 113. At the same time it provides Content Provider(s) 101 a level of assurance that their digital assets are protected and monitored so that they can receive appropriate compensation for the licensing of Content 113.

II. CRYPTOGRAPHY CONCEPTS AND THEIR APPLICATION TO THE SECURE DIGITAL CONTENT ELECTRONIC DISTRIBUTION SYSTEM

[0050] License Control in the Secure Digital Content Electronic Distribution System 100 is based on the use of cryptography. This section introduces basic cryptography technologies of the present invention. The use of public key encryption, symmetric key encryption, digital signatures, digital watermarks and digital certificates is known.

A. Symmetric Algorithms

[0051] In the Secure Digital Content Electronic Distribution System 100 the Content Provider(s) 101 encrypts the content using symmetric algorithms. They are called symmetric algorithms because the same key is used to encrypt and decrypt data. The data sender and the message recipient must share the key. The shared key is referred to here as the symmetric key. The Secure Digital Content Electronic Distribution System 100 architecture is independent of the specific symmetric algorithm selected for a particular implementation.

[0052] Common symmetric algorithms are DES, RC2 and RC4. Both DES and RC2 are block cipher. A block cipher encrypts the data using a block of data bits at a time. DES is an official US government encryption standard, has a 64-bit block size, and uses a 56-bit key. Triple-DES is commonly used to increase the security achieved with simple DES. RSA Data Security designed RC2. RC2 uses a variable-key-size cipher and has a block size of 64 bits. RC4, also designed by RSA Data Security, is a variable-key-size stream cipher. A stream cipher operates on a single bit at a time. RSA Data Security claims that eight to sixteen machine operations are required for RC4 per output byte.

[0053] IBM designed a fast algorithm called SEAL. SEAL is a stream algorithm that uses a variable-length key and that has been optimized for 32-bit processors. SEAL requires about five elementary machine instructions per data byte. A 50-MHz, 486-based computer runs the SEAL code at 7.2 megabytes/second if the 160-bit key used has already been preprocessed into internal tables.

[0054] Microsoft reports results of encryption performance benchmark in its Overview of Cryptographic document. These results were obtained by an application using Microsoft's CryptAPI, running on a 120-MHz, Pentium-based computer

with Windows NT 4.0.

certificate, the recipient of the message uses the entity's name from the certificate to decide whether or not to accept the message.

Cipher	Key Size	Key Setup Time	Encryption Speed
DES	64	460	1138519
RC2	40	40	208888
RC4	40	151	2377723

10 **B. Public Key Algorithms**

[0053] In the Secure Digital Content Electronic Distribution System 100, symmetric keys and other small data pieces

are encrypted using public keys. Public key algorithms use two keys. The two keys are mathematically related so that data encrypted with one key can only be decrypted with the other key. The owner of the keys keeps one key private (private key) and publicly distributes the second key (public key).

[0054] To ensure the transmission of a confidential message using a public key algorithm, one must use the recipient's public key to encrypt the message. Only the recipient, who has the associated private key, can decrypt the message. Public key algorithms are also used to generate digital signatures. The private key is used for that purpose.

[0055] The most common public-key algorithm is the RSA public-key cipher. It has become the de-facto public key standard in the industry. Other algorithms that also work well for encryption and digital signatures are ElGamal and Rubin. RSA is a variable-key length cipher.

[0056] Symmetric key algorithms are much faster than the public key algorithms. In software, DES is generally at least 100 times as fast as RSA. Because of this, RSA Data Security's toolkit BSAFE 3.0 has a throughput for private-key operations (encryption or decryption, using the private key) of 21.9 kilobit/second with a 512-bit modulus and 7.4 kilobit/second with a 1024-bit modulus.

11 **C. Digital Signature**

[0057] In the Secure Digital Content Electronic Distribution System 100, the issuer of SC(e) protects the integrity of SC(e) by digitally signing it. In general, a message owner first computes the message digest (defined below) and then encrypts the digital signature of a message, a message owner first computes the message digest (defined below) and then encrypts the digital signature of the message using the owner's private key. The message is distributed with its signature. Any recipient of the message can verify the digital signature first by decrypting the signature using the public key of the message owner to recover the message digest. Then, the recipient computes the digest of the received message and compares it with the recovered one. If the message has not been altered during distribution, the calculated digest and recovered digest must be equal.

[0058] In the Secure Digital Content Electronic Distribution System 100, since SC(e) contain several data parts, a digest is calculated for each part and a summary digest is calculated for the concatenated part digests. The summary digest is encrypted using the private key of the issuer of the SC(e). The encrypted summary digest is the issuer's digital signature for the SC(e). The part digests and the digital signature are included in the body of the SC(e). The recipient of SC(e) can verify the integrity of the SC(e) and its parts by means of the received digital signature and part digests.

[0059] A one-way hash algorithm is used to calculate a message digest. A hash algorithm takes a variable-length input message and converts it into a fixed length string, the message digest. A one-way hash algorithm operates only in one direction. That is, it is easy to calculate the digest for an input message, but it is very difficult (computationally infeasible) to generate the input message from its digest. Because of the properties of the one-way hash functions,

[0060] The most common one-way hash functions are MD5 from RSA Data Security and SHA designed by the US National Institute of Technology and Standards (NITS).

12 **Digital Certificates**

[0061] A digital certificate is used to authenticate or verify the identity of a person or entity that has sent a digitally signed message. A certificate is a digital document issued by a certification authority that binds a public key to a person or entity. The certificate includes the public key, the name of the person or entity, an expiration date, the name of the certification authority, and other information. The certificate also contains the digital signature of the certification authority.

[0062] When an entity (or person) sends a message signed with its private key and accompanied with its digital

certificate, the recipient of the message uses the entity's name from the certificate to decide whether or not to accept the message.

[0063] In the Secure Digital Content Electronic Distribution System 100, every SC(e), except those issued by the End-User Device(s) 109, includes the certificate of the creator of the SC(e). The End-User Device(s) 109 do not need to include certificates in their SC(e)s because many End-User(s) do not bother to acquire a certificate or have certificates issued by non-bona-fide Certification Authorities. In the Secure Digital Content Electronic Distribution System 100, the Clearinghouse(s) 108 has the option of issuing certificates to the Electronic Digital Content Store(s) 103. This allows the End-User Device(s) 109 to independently verify that the Electronic Digital Content Store(s) 103 have been authorized by the Secure Digital Content Electronic Distribution System 100.

13 **E. Guide To The SC(e) Graphical Representation**

[0064] This document uses a drawing to graphically represent SC(e) that shows encrypted parts, non-encrypted parts, the encryption keys, and certificates. Referring now to FIG. 2 is an example drawing of SC(e) 200. The following symbols are used in the SC(e) figures. Key 201 is a public or private key. The length of the key e.g., CLRUGH for Clearinghouse, indicate the key owner. PB 202 is the handle indicates that it is a public key than key 201 is a Clearinghouse public key. PV 203 is the handle indicates that it is a private key. Diamond shape is an End-User Digital Signature 202. The initials indicate which private key was used to create the signature thus in EU is the End-User's digital signature from table below. Symmetric key 203 is used to encrypt content. An encrypted symmetric key object 204, comparable a symmetric key 203 encrypted with a PB of CLRUGH. The key on the top border of the rectangle is the key used in the encryption of the object. The symbol or text inside the rectangle indicates the encrypted object (a symmetric key in this case). Another encrypted object, in this example a Transaction ID encrypted object 205 is shown. And Usage Conditions 206 for content licensing management as described below. The SC(e) 200 comprises Usage Conditions 208, Transaction ID encrypted object 205, an Application ID encrypted object 207, and encrypted symmetric key object 204, all signed by an End-User Digital Signature 202.

[0065] The table below shows the initials that identify the signer of SC(e).

Initial	Component
CP	Content Provider(s) 101
MS	Electronic Digital Content
HS	Content Hosting Site(s) 111
EU	End-User Device(s) 109
CH	Clearinghouse(s) 108
CA	Certification authority(s)

14 **F. Example of a Secure Container Encryption**

[0066] The tables and diagrams below provide an overview of the encryption and decryption process used to create and recover information from SC(e)s. The SC(e)s that is created and decrypted in this process overview is a general SC (e). It does not represent any of the specific SC(e)s types used for rights management in the Secure Digital Content Electronic Distribution System 100. The process consists of the steps described in FIG. 3 for encryption process.

[0067] Process Flow for Encryption Process of FIG. 3

Step	Process
301	Sender generates a random symmetric key and uses it to encrypt the content.
302	Sender runs the encrypted content through a hash algorithm to produce the content digest.
303	Sender encrypts the symmetric key using the recipient's public key. PB RECPNT refers to the recipient's public key.
304	Sender runs the encrypted symmetric key through the same hash algorithm used in step 2 to produce the symmetric key digest.
305	Sender runs the concatenation of the content digest and symmetric key digest through the same hash algorithm used in step 2 to produce the SC(e) digest.

(continued)

Step	Process
308	Sender encrypts the SC(s) digest with the sender's private key to produce the digital signature for the SC (a). PV SENDER refers to the sender's private key.
307B	Sender creates a SC(s) file that includes the encrypted content, encrypted symmetric key, content digest, symmetric key digest, sender's certificate, and SC(s) signature.
307A	Sender must have obtained the certificate from a certification authority prior to initiating secure communications. The certification authority includes in the certificate the sender's public key. Sender transmits the SC name and signs it. PV CAUTHR refers to the certifications authority's private key. Sender transmits the SC (a) to the recipient.

[0070] Process Flow for Decryption Process of FIG. 4

Step	Process
408	Recipient receives the SC(s) and separates its parts.
409	Recipient verifies the digital signature in the sender's certificate by decrypting it with the public key of the certification authority. If the certificate's digital signature is valid, recipient acquires the sender's public key from the certificate.
410	Recipient decrypts the SC(s) digital signature using the sender's public key. This recovers the SC(s) digest. PB SENDER refers to the sender's public key.
411	Recipient runs the concatenation of the received content digest and encrypted key digest through the same hash algorithm used by the sender to compute the SC(s) digest.
412	Recipient compares the computed SC(s) digest with the one recovered from the sender's digital signature. If they are the same, recipient confirms that the received digests have not been altered and continues with the decryption process. If they are not the same, recipient discards the SC(s) and notifies the sender.
413	Recipient runs the encrypted symmetric key through the same hash algorithm used in step 411 to compute the symmetric key digest.
414	Recipient compares the computed symmetric key digest with the one received in the SC(s). If it is the same, recipient knows that the encrypted symmetric key has not been altered. Recipient continues with the decryption process. If not valid, recipient discards the SC(s) and notifies the sender.
415	Recipient runs the encrypted content through the same hash algorithm used in step 411 to compute the content digest.
416	Recipient compares the computed content digest with the one received in the SC(s). If it is the same, recipient knows that the encrypted content has not been altered. Recipient then continues with the decryption process. If not valid, recipient discards the SC(s) and notifies the sender.
417	Recipient decrypts the encrypted symmetric key using the recipient's private key. This recovers the symmetric key. PV RECIPIENT refers to the recipient's private key.
418	Recipient uses the symmetric key to decrypt the encrypted content. This recovers the content.

III. SECURE DIGITAL CONTENT ELECTRONIC DISTRIBUTION SYSTEM FLOW

45	[0071] The Secure Electronic Digital Content Distribution System 100, consists of several components that are used by the different participants of the system. These participants include the Content Provider(s) 101, Electronic Digital Content Store(s) 103, End-User Device(s) 109, and the Clearinghouse(s) 105. A high level system flow is used as an overview of the Secure Digital Content Electronic Distribution System 100. This flow outlined below tracks Content as it flows throughout the System 100. Additionally it outlines the steps used by the participants to conduct the transactions for the purchase, unblocking and use of the Content 113. Some of the assumptions made in the system flow include:
46	This is a system flow for a Digital Content service (Point-to-Point Interface to a PCI).
47	Content Provider(s) 101 submits audio Digital Content in PCM uncompressed format (as a music audio example).
48	Content Provider(s) 101 has metadata in an ODBC compliant database or Content Provider(s) 101 will enter the data directly into the Content Information Processing Subsystem, or will have provided data in prescribed ASCII file format(s).

Financial settlement is done by the Electronic Digital Content Store(s). Content 113 is hosted at a single Content Hosting Site(s).

Content 113 is hosted at a single Content Hosting Site(s).

the exact nature of the Digital Content e.g. music, video and program and electronic distribution systems broadcast.

5

[0072] It should be understood by those skilled in the art that these assumptions can be altered to accommodate the exact nature of the Digital Content e.g. music, video and program and electronic distribution systems broadcast.

6

[0073] The following process flow is illustrated in FIG. 1.

Step	Process
10	A uncompRESSED PCM audio file is provided as Content 113 by the Content Provider(s) 101 unique identifier for the Content 113.
121	The Work Flow Manager Tool 134 is used to direct the content flow through the acquisition and preparation process at the Content Provider(s) 101. It can also be used to track the status of any piece of content in the system at any time.
122	Metadata is captured from the Content Provider(s) 101 unique identifier for the Content 113 and information provided by the Database Mapping Template.
123	The Work Flow Manager Tool 134 is used to direct the content flow through the acquisition and preparation process at the Content Provider(s) 101. It can also be used to track the status of any piece of content in the system at any time.
124	The Usage Conditions for the Content 113 are entered into the Content Information Processing Subsystem. This can be done either manually or automatically. This data includes copy restriction rules and any other business rules deemed necessary. All of the metadata entry can occur in parallel with the Audio Processing for the data.
125	The Watermarking Tool is used to hide data in the Content 113 that the Content Provider(s) 101 deems necessary to identify the content. This could include when it was captured, where it came from (the Content Provider(s) 101), or any other information specified by the Content Provider(s) 101.
126	The Usage Conditions for the Content 113 are entered into the Content Information Processing Subsystem. This can be done either manually or automatically. This data includes copy restriction rules and re-sampling to the Content 113 as necessary for the different compression levels supported.
127	The Content 113 is compressed using the Content Processing Tool 125 to the desired compression levels. The Content 113 can then be played back to verify that the compression produces the required level of quality. If necessary the equalization, dynamics adjustments, compression and playback quality checks can be performed as many times as desired.
128	The Content 113 and a subset of its metadata is encrypted with a Symmetric Key by the SC Packager. This tool then encrypts the key using the Public Key of the Clearinghouse(s) 105 to produce an Encrypted Symmetric Key. This key can then be transmitted anywhere without compromising the security of the Content 113 since the only entity that can decrypt it is the Clearinghouse(s) 105.
129	The Encrypted Symmetric Key, metadata and other information about the Content 113 is then packed into a Metadata SC by the SC Packager Tool 152.
130	The encrypted Content 113 and metadata are then packed into a Content SC. At this point the processing on the Content 113 and metadata is complete.
131	The Metadata SC(s) is then sent to the Content Promotions Web Site 158 using the Content Disbursement Tool (not shown).
132	The Content Disbursement Tool sends the Content SC(s) to the Content Hosting Site(s) 111. The Content Hosting Site(s) can reside at the Content Provider(s) 101, the Clearinghouse(s) 105 or a special location dedicated for Content Hosting. The URL for this site is part of the metadata that was added to the Metadata SC.
133	The Content Promotions Web Site 158 notifies Electronic Digital Content Store(s) 103 of new Content 113 that is added to the System 100.
134	Using the Content Acquisition Tool, Electronic Digital Content Store(s) 103 then download the Metadata SC(s) that correspond to the Content 113 they wish to sell.
135	The Electronic Digital Content Store(s) 103 will use the Content Acquisition Tool to pull out any data from the Metadata SC(s) that they want to use to promote the Content 113 on their Web Site. Access to portions of this metadata can be secured and charged if desired.
136	The Usage Conditions for the Content 113, specific to this Electronic Digital Content Store(s) 103, are entered using the Content Acquisition Tool. These Usage Conditions include the retail price and copy/
137	restrictions for the different compression levels of the Content 113.

(continued)

Step	Process
134	The Electronic Digital Content Store(s) 103 receives Usage Conditions and the original Metadata SC(s) are packed into an Offer SC by the SC Packer Tool.
135	After the Electronic Digital Content Store(s) 103 web Site is updated, the Content 113 is available to End-User(s) surfing the Web.
136	When an End-User(s) finds Content 113 that they want to buy, they click on a content icon, such as a music icon, and the item is added to their shopping cart which is maintained by the Electronic Digital Content Store(s) 103, when the End-User(s) completes shopping they submit the purchase request to the Electronic Digital Content Store(s) 103 for processing.
137	The Electronic Digital Content Store(s) 103 then interacts with credit card clearing organizations to place a hold on the funds in the same way they do business today.
138	Once the Electronic Digital Content Store(s) 103 receives the credit card authorization number back from the credit card clearing organization, it stores that into a database and invokes the SC Packer Tool to build a Transaction SC. This Transaction SC includes all of the Offer SCs for the Content 113 that the End-User(s) has purchased, a Transaction ID that can be tracked back to the Electronic Digital Content Store(s) 103, information that identifies the End-User(s), compensation levels, Usage Conditions and the price list for the songs purchased.
139	The Transaction SC is then transmitted to the End-User Device(s) 109.
140	When the Transaction SC arrives on the End-User Device(s) 109, it ticks off the End-User Player Application 108, which opens the Transaction SC and acknowledges the End-User's purchase. The End-User Player Application 108 then opens the individual Offer SCs and in an alternate embodiment, may inform the user with an estimate of the download time. It then asks the user to specify when they want to download the Content 113.
141	Based on the time the End-User(s) requested the download, the End-User Player Application 108 will wake up and initiate the start of the download process by building a Offer SC that contains among other things the Encrypted Symmetric Key for the Content 113, the Transaction ID, and End-User(s) information.
142	The Order SC is then sent to the Clearinghouse(s) 105 for processing.
143	The Clearinghouse(s) 105 receives the Order SC, opens it and verifies that none of the data has been tampered with. The Clearinghouse(s) 105 validates the Usage Conditions purchased by the Content Provider(s) 101. This information is logged in a database.
144	Once all the checks are complete, the Encrypted Symmetric Key is decrypted using the private key of the Clearinghouse(s) 105. The Symmetric Key is then encrypted using the public key of the End-User(s). This new Encrypted Symmetric Key is then packaged into a License SC by the SC Packer.
145	The License SC is then transmitted to the End-User(s).
146	When the License SC is received at the End-User Device(s) 109 it is stored in memory until the Content SC is downloaded.
147	The End-User Device(s) 109 request from the Content Hosting Facility 111, sending the corresponding License SC for the purchased Content 113.
148	Content 113 is sent to the End-User Device(s) 109. Upon the receipt the Content 113 is de-encrypted by the End-User Device(s) 109 using the Symmetric Key.
45	

IV. RIGHTS MANAGEMENT ARCHITECTURE MODEL

A. Architecture Layer Functions

[0074] FIG. 5 is a block diagram of the Rights Management Architecture of the Secure Digital Content Electronic Distribution System 100. Architecturally, four layers represent the Secure Digital Content Electronic Distribution System 100, the License Control Layer 501, the Content Identification Layer 503, Content Usage Control Layer 505, and the Content Formatting Layer 507. The overall functional objective of each layer and the individual key functions for each layer are described in this section. The functions in each of the layers are fairly independent of the functions in the other layers. Within broad limitations, functions in a layer can be substituted with similar functions without affecting the functionality of the other layers. Obviously, it is required that the output from one layer matches format and semantics acceptable to the adjacent layer.

[0075] The License Control Layer 501 ensures that:

- the Digital Content is protected during distribution against illegal interception and tampering;
- the Content 113 originates from a legal content owner and is distributed by a licensed distributor, e.g. Electronic Digital Content Store(s) 103;
- the Digital Content purchaser has a properly licensed application;
- the distributor is paid by the purchaser before a copy of the Content 113 is made available to the purchaser or a record of the transaction is kept for reporting purposes.

[0076] The Content Identification Layer 503 allows for the verification of the copyright and the identity of the content purchaser. The content's copyright information and identity of the content purchaser enables the source tracking of any, authorized or not, copy of Content 113. Thus the Content Identification Layer 503 provides a means to combat piracy.

[0077] The Content Usage Control Layer 505 ensures that the copy of the Content 113 is used in the purchaser's device according to the Store Usage Conditions 519. The Store Usage Conditions 519 may specify in the purchaser's plays and local copies allowed for the Content 113, and whether or not the Content 113 may be recorded to an external portable device. The functions in the Content Usage Control Layer 505 keep track of the content's copy/play usage and update the copy/play status.

[0078] The Content Formatting Layer 507 allows for the format conversion of the Content 113 from its native representation in the content owner's facilities into a form that is consistent with the service features and distribution means encoding and its associated preprocessing, such as frequency equalization and amplitude dynamic adjustment. For Content 113 which is audio, at the purchaser's side, the received Content 113 also needs to be processed to achieve a format appropriate for playback or transfer to a portable device.

B. Function Partitioning and Flows

[0079] The Rights Management Architectural Model is shown in FIG. 5 and this illustrates the mapping of the architectural layers to the operating components making up the Secure Digital Content Electronic Distribution System 100 and the key functions in each layer.

1. Content Formatting Layer 507

[0080] The general functions associated with the Content Formatting Layer 507 are Content Preprocessing 502 and Compensation 511 at the Content Provider(s) 101, and Content De-scrambling 513 and Decompression 515 at the End-User Device(s) 109. The need for preprocessing and the examples of specific functions were mentioned above. Content Compensation 511 is used to reduce the file size of the Content 113 and its transmission time. Any compression algorithm appropriate for the type of Content 113 and transmission medium can be used in the Secure Digital Content Electronic Distribution System 100. For Music, MP3/MP4, Dolby AC-2 and AC-3, Sony Adaptive Transform Coding (ATRAC), and low-bit-rate algorithms are some of the typically used compression algorithms. The Content 113 is stored in the End-User Device(s) 109 in compressed form to reduce the storage size requirement. It is decompressed during active playback. De-scrambling is also performed during active playback. The purpose and type of scrambling will be described later during the discussion of the Content Usage Control Layer 505.

2. Content Usage Control Layer 505

[0081] The Content Usage Control Layer 505 permits the specification and enforcement of the conditions of restriction imposed on the use of Content 113 at the End-User Device(s) 109. The conditions may specify the number of plays allowed for the Content 113, whether or not a secondary copy of the Content 113 is allowed, the number of secondary copies, and whether or not the Content 113 may be copied to an external portable device. The Content Provider(s) 101 sets the applicable Usage Conditions 517 and transmits them to the Electronic Digital Content Store(s) 103 (see the License Control Layer 501 section). The Electronic Digital Content Store(s) 103 can add to or narrow the Usage Conditions 517 as long as it doesn't invalidate the original conditions set by the Content Provider(s) 101. The Electronic Digital Content Store(s) 103 then transmits all Store Usage Conditions 519 (in a SC) to the End-User Device(s) 109 and the Clearinghouse(s) 105. The Clearinghouse(s) 105 perform Usage Conditions Validation 521 before authorizing the Content 113 release to an End-User Device(s) 109.

[0082] The enforcement of the content Usage Conditions 517 is performed by the Content Usage Control Layer 505

In the End-User Device(s) 109. First, upon reception of the Content 113 copy from the Content Identification Layer 503 in the End-User Device(s) 109 marks the Content 113 with a Copy/Play Code 523 representing the initial copy/permision. Second, the Player Application 198 cryptographically scrambles the Content 113 before storing it in the End-User Device(s) 109. The Player Application 198 generates a scrambling key for such Content item, and the key is encrypted and hidden in the End-User Device(s) 109. Then, every time the End-User Device(s) 109 accesses the Content 113 for copy or play, the End-User Device(s) 109 verifies the copy/play code before allowing the de-scrambling of the Content 113 and the execution of the play or copy. The End-User Device(s) 109 also appropriately updates the copy/play code in the original copy of the Content 113 and on any new secondary copy. The copy/play coding is performed on Content 113 that has been compressed. That is, there is no need to decompress the Content 113 before the embedding of the copy/play code.

[0083] The End-User Device(s) 109 uses a License Watermark 527 to embed the copy/play code within the Content 113. Only the End-User Player Application 198 that is knowledgeable of the embedding algorithm and the associated scrambling key is able to read or modify the embedded data. The data is invisible or inaudible to a human observer, that is, the data introduces no perceivable degradation to the Content 113. Since the watermark survives several steps of content processing, data compression, D-to-H and A-to-D conversion, and signal degradation introduced by normal content handling, the watermark stays with the Content 113 in any representation form, including analog representation. In an alternate embodiment, instead of using a License Watermark 527 to embed the copy/play code within the Content 113, the End-User Player Application 198 uses securely stored Usage Conditions 519.

20 3. Content Identification Layer 503

[0084] As part of the Content Identification Layer 503, the Content Provider(s) 101 also uses a License Watermark 527 to embed data in the Content 113 such as to the content identifier, content owner and other information, such as publication date and geographic distribution region. This watermark is referred to here as the Copyright Watermark 529. Upon reception, the End-User Device(s) 109 watermarks the copy of the Content 113 with the content purchaser's name and the Transaction ID 535 (see the License Control Layer 501 section below), and with other information such as date of license and Usage Conditions 517. This watermark is referred to here as the license watermark. Any copy or Content 113, obtained in an authorized manner or not, and subject to audit processing that preserves the content quality, carries the copyright and license watermarks. The Content Identification Layer 503 defers piracy.

4. License Control Layer 501

[0085] The License Control Layer 501 protects the Content 113 against unauthorized interception and ensures that the Content is only released on an individual basis to an End-User(s) that has properly licensed End-User Device(s) 109 and subsequently completes a license purchase transaction with an authorized Electronic Digital Content Store(s) 103. The License Control Layer 501 protects the Content 113 by double Encryption 531. The Content 113 is encrypted using an encryption symmetric key generated by the Content Provider(s) 101, and the symmetric key is encrypted using the public key 621 of the Clearinghouse(s) 105. Only the Clearinghouse(s) 105 can initially recover the symmetric key. [0086] License control is designed with the Clearinghouse(s) 105 as the 'trusted party'. Before releasing permission for the License Request 537, (i.e., the Symmetric Key 623 for the Content 113 to an End-User Device(s) 109), the Clearinghouse(s) 105 verifies that the Transaction 541 and the License Authorization 543 are complete and authentic, that the Electronic Digital Content Store(s) 103 has authorization from the Secure Digital Content Electronic Distribution System 100 for the sale of electronic Content 113, and that the End-User(s) 109 has a properly licensed application. Audit Reporting 545 allows the generation of reports and the sharing of licensing transaction information with other authorized parties in the Secure Electronic Digital Content Distribution System 100.

[0087] License control is implemented through SC Processing 533. SC(s) are used to distribute encrypted Content 113 and information among the system operation components (more on the SC(s) detailed structure sections below). A SC is a cryptographic container of information that uses cryptographic encryption, digital signatures and digital certificates to provide protection against unauthorized manipulation and modification of the electronic information or Content 113. It also allows for the authentic verification of the electronic data.

[0088] License control requires that the Content Provider(s) 101, the Electronic Digital Content Store(s) 103 and the Clearinghouse(s) 105 have bona fide cryptographic digital certificates from reputable Certificate Authorities that are used to authenticate those components. The End-User Device(s) 109 are not required to have digital certificates.

5. Content Distribution and Licensing Control

[0089] FIG. 8 is a block diagram illustrating an overview of the Content Distribution and Licensing Control as it applies to the License Control Layer of FIG. 5. The figure depicts the case in which the Electronic Digital Content Store(s) 103,

End-User Device(s) 109 and the Clearinghouse(s) 105 are interconnected via the Internet, and unicast (point-to-point) transmission is used among those components. The communication between the Content Provider(s) 101 and the Electronic Digital Content Store(s) 103 could also be over the Internet or other network. It is assumed that the Content purchase commercial transaction between the End-User Device(s) 109 and the Electronic Digital Content Store(s) 103 is based on standard Internet Web protocols. As part of this Web-based interaction, the End-User(s) makes the selection of the Content 113 to purchase, provides personal and financial information, and agrees to the conditions of purchase.

The Electronic Digital Content Store(s) 103 could obtain payment authorization from an acquirer institution using a protocol such as SET.

[0090] It is also assumed in FIG. 8 that the Electronic Digital Content Store(s) 103 has downloaded the End-User Player Application 198 to an End-User Device(s) 109 based on standard Web protocols. The architecture requires that, the Electronic Digital Content Store(s) 103 assumes a unique identifier ID to the downloaded Player Application 198 and that the End-User Device(s) 109 stores ID for later application license verification (see below).

[0091] The overall licensing flow starts at the Content Provider(s) 101. The Content Provider(s) 101 encrypts the Content 113 using an encryption symmetric key locally generated, and encrypts the Symmetric Key 623 using the Clearinghouse(s) 105 public key 621. In an alternate embodiment, the symmetric key instead of being locally generated may be sent to the Content Provider(s) 101 from the Clearinghouse(s) 105. The Content Provider(s) 101 creates a Content SC(s) 630 around the encrypted Content 113, and a Metadata SC(s) 620 around the encrypted Symmetric Key 623, Store Usage Conditions 519, and other Content 113 associated information. There is one Metadata SC(s) 620 and one Content SC(s) 630 for every Content 113 object. The Content 113 object may be a composition level one same song or the Content 113 object may be each song on the album. The Content 113 object may be the entire album. For each Content 113 object, the Metadata SC(s) 620 also carries the Store Usage Conditions 519 associated with the Content Usage Control Layer 505.

[0092] The Content Provider(s) 101 distributes the Metadata SC(s) 620 to one or more Electronic Digital Content Store(s) 103 (step 601) and the Content SC(s) 630 to one or more Content Holding Sites (step 602). Each Electronic Digital Content Store(s) 103, in turn creates an Offer SC(s) 641. The Offer SC(s) 641 typically carries much of the same information as the Metadata SC(s) 620, including the Digital Signature 624 of the Content Provider(s) 101 and the Certificate (not shown) of the Content Provider(s) 101. As mentioned above, the Electronic Digital Content Store 603 can add to or narrow the Store Usage Conditions 519 (handled by the Control Usage Control Layer) initially defined by the Content Provider(s) 101. Optionally, the Content SC(s) 630 and/or the Metadata SC(s) 620 is signed with a Digital Signature 622 of the Content Provider(s) 101.

[0093] After the completion of the Content-purchase transaction between the End-User Device(s) 109 and the Electronic Digital Content Store(s) 103 (step 603) the Electronic Digital Content Store(s) 103 creates and transmits to the End-User Device(s) 109 a Transaction SC(s) 640 (step 604). The Transaction SC(s) 640 includes a unique Transaction ID 635, the purchaser's name (i.e., End-User(s)) (not shown), the Public Key 681 of the End-User Device(s) 109, and the Offer SC(s) 641 associated with the purchased Content 113. The Transaction Data 642 in FIG. 8 represents both the Transaction ID 635 and the End-User(s) name (not shown). The Transaction Data 642 is encrypted with the Public Key 621 of the Clearinghouse(s) 105. Optionally, the Transaction SC(s) 640 is signed with a Digital Signature 643 of the Electronic Digital Content Store(s) 103.

[0094] Upon reception of the Transaction SC(s) 640 (and the Offer SC(s) 641 included in it), the End-User Player Application 198 running on End-User Device(s) 109 solicits license authorization from the Clearinghouse(s) 105 by means of an Order SC(s) 650 (step 605). The Order SC(s) 650 includes the encrypted Symmetric Key 623 and Store Usage Conditions 519 from the Offer SC(s) 641, the encrypted Transaction Data 642 from the Transaction SC(s) 640, and the encrypted Application ID 651 from the End-User Device(s) 109. In another embodiment, the Order SC(s) 650 is signed with a Digital Signature 652 of the End-User Device(s) 109.

[0095] Upon reception of the Order SC(s) 650 from the End-User Device(s) 109, the Clearinghouse(s) 105 verifies:

1. that the Electronic Digital Content Store(s) 103 has authorization from the Secure Digital Content Electronic Distribution System 100 (exists in the Database 160 of the Clearinghouse(s) 105);
2. that the Order SC(s) 650 has not been altered;
3. that the Order SC(s) 650 has not been altered;
4. that the electronic Store Usage Conditions 519 purchased by the End-User Device(s) 109 are consistent with those Usage Conditions 517 held by the Content Provider(s) 101; and
5. that the Application ID 651 has a valid structure and that it was provided by an authorized Electronic Digital Content Store(s) 103.

[0096] If the verifications are successful, the Clearinghouse(s) 105 decrypts the Symmetric Key 623 and the Transaction Data 642 and builds and transfers the License SC(s) 660 to the End-User Device(s) 109 (step 606). The License SC(s) 660 carries the Symmetric Key 623 and the Transaction Data 642, both encrypted using the Public Key 681 of

the End-User Device(s) 109, if any verification is not successful, the Clearinghouse(s) 105 denies the license to the End-User Device(s) 109 and informs the End-User Device(s) 109. The Clearinghouse(s) 105 also immediately informs the Electronic Digital Content Store(s) 103 of the verification failure. In an alternate embodiment, the Clearinghouse (s) 105 signs the License SC(s) 860 with its Digital Signature 863.

[0087] After receiving the License SC(s) 860, the End-User Device(s) 109 decrypts the Symmetric Key 823 and the Transaction Data 842 previously received from the Clearinghouse(s) 105 and requests the Content SC(s) 830 (step 607) from a Content Hosting Site(s) 111. Upon arrival of the Content SC(s) 830 (step 608), the End-User Device(s) 109 decrypts the Content 113 using the Symmetric Key 823 (step 609), and passes the Content 113 and the Transaction Data 842 to the other layers for license watermarking, copy/play coding, scrambling, and further Content 113 processing as described previously for FIG. 5.

[0088] Finally, the Clearinghouse(s) 105 on a periodic basis transmits summary transaction reports to the Content Provider(s) 101 and the Electronic Digital Content Store(s) 103 for auditing and tracking purposes (step 610).

V. SECURE CONTAINER STRUCTURE

A. General Structure

[0089] A Secure Container (SC) is a structure that consists of several parts which together define a unit of Content 113 or a portion of a transaction, and which also define related information such as Usage Conditions, metadata, and encryption methods. SC(s) are designed in such a way that the integrity, completeness, and authenticity of the information can be verified. Some of the information in SC(s) may be encrypted so that it can only be accessed after proper authorization has been obtained.

[0100] SC(s) include at least one bill of materials (BOM) part which has records of information about the SC(s) and about each of the parts included in the SC(s). A message digest is calculated, using a hashing algorithm such as MD5, for each part and then included in the BOM record for the part. The digests of the parts are concatenated together and another digest is computed from them and then encrypted using the private key of the entity creating the SC(s) to create a digital signature. Parties holding the SC(s) can use the digital signature to verify all of the digests and thus validate the integrity and completeness of the SC(s) and all of its parts.

[0101] The following information may be included as records in the BOM along with the records for each part. The SC(s) type determines which records need to be included:

- SC(s) ID
- Type of SC(s) (e.g. Offer, Order, Transaction, Content, Metadata or promotional and License.)
- Publisher of the SC(s)
- Data that the SC(s) was created
- Expiration date of the SC(s)
- Description of the algorithm used for the digital signature encryption (default is RSA)
- Description of the digest algorithm used for the included parts (default is MD5)
- Clearinghouse(s) URL
- Description of the digest algorithm used for the concatenated digests of the included parts
- Digital signature (encrypted digest of all of the concatenated digests of the included parts)

[0102] SC(s) may include more than one BOM. For example, an Offer SC(s) 841 consists of the original Metadata SC(s) 820 parts, including its BOM, as well as additional information added by the Electronic Digital Content Store(s) 103 and a new BOM. A record for the Metadata SC(s) 820 BOM is included in the Offer SC(s) 841 BOM. This record includes a digest for the Metadata SC(s) 820 BOM which can be used validate its integrity and therefore, the integrity of the parts included from the Metadata SC(s) 820 can also be validated using the part digest values stored in Metadata SC(s) 820. None of the parts from the Metadata SC(s) 820 have records in the new BOM that was created for the Offer SC(s) 841. Only parts added by the Electronic Digital Content Store(s) 103 and the Metadata SC(s) 820 BOM have records in the new BOM.

[0103] SC(s) may also include a Key Description part. Key Description parts include records that contain the following information about encrypted parts in the SC(s):

- The name of the encrypted part.
- The name to use for the part when it is decrypted.
- The encryption algorithm used to encrypt the part.
- Either a Key Identifier to indicate the public encryption key that was used to encrypt the part or an encrypted symmetric key that, when decrypted, is used to decrypt the encrypted part.

The encryption algorithm used to encrypt the symmetric key. This field is only present when the record in the Key Description part includes an encrypted symmetric key that was used to encrypt the encrypted part. A Key Identifier of the symmetric key that was used to encrypt the encrypted part.

[0104] If the SC(s) does not contain any encrypted parts, then there is no Key Description part.

B. Rights Management Language Syntax and Semantics

[0105] The Rights Management Language consists of parameters that can be assigned values to define restrictions on the use of the Content 113 by an End-User(s) after the Content 113 purchase. The restrictions on the use of the Content 113 is the Usage Conditions 517. Each Content Provider(s) 101 specifies the Usage Conditions 517 for each of its Content 113 items. Electronic Digital Content Store(s) 103 interpret the Usage Conditions 517 in Metadata SC(s) 820 and use the information to provide select options they wish to offer their customers as well as additional purchase information for the Content 113. After an End-User(s) has selected a Content 113 item for purchase, the End-User Device(s) 109 requests authorization for the Content 113 based on Store Usage Conditions 518. Before the Clearinghouse(s) 105 sends a License SC(s) 860 to the End-User(s), the Clearinghouse(s) 105 verifies that the Store Usage Conditions 518 being requested are in agreement with the allowable Usage Conditions 517 that were specified by the Content Provider(s) 101 in the Metadata SC(s) 820.

[0106] When an End-User Device(s) 109 receives the Content 113 that was purchased, the Store Usage Conditions 518 are encoded into that Content 113 using the Watermarking Tool or encoded in the securely stored Usage Conditions 518. The End-User Player Application 195 running on End-User Device(s) 109 insure that the Store Usage Conditions 519 that were encoded into the Content 113 are enforced.

[0107] The following are examples of Store Usage Conditions 519 for an embodiment where the Content 113 is music:

- Song is recordable.
- Song can be played in number of times.

C. Overview of Secure Container Flow and Processing

[0108] Metadata SC(s) 820 are built by Content Provider(s) 101 and are used to define Content 113 items such as songs. The Content 113 itself is not included in these SC(s) because the size of the Content 113 is typically too large for Electronic Digital Content Store(s) 103 and End-User(s) to efficiently download the container just for the purpose of accessing the descriptive metadata. Instead, the SC(s) includes an external URL (Uniform Resource Locator) to point to the Content 113. The SC(s) also includes metadata that provides descriptive information about the Content 113 and any other associated data, such as for music, the CD cover art and/or digital audio clips in the case of song content 113.

[0109] Electronic Digital Content Store(s) 103 download the Metadata SC(s) 820, for which they are authorized, and build Offer SC(s) 841. In short, an Offer SC(s) 841 consists of some of the parts and the BOM from the Metadata SC(s) 820 along with additional information included by the Electronic Digital Content Store(s) 103. A new BOM for the Offer SC(s) 841 is created when the Offer SC(s) 841 is built. Electronic Digital Content Store(s) 103 also use the Metadata SC(s) 820 by extracting metadata information from them to build HTML pages on their web sites that present descriptions of Content 113 to End-User(s), usually so they can purchase the Content 113.

[0110] The information in the Offer SC(s) 841 that is added by the Electronic Digital Content Store(s) 103 is typically to narrow the selection of Usage Conditions 517 that are specified in the Metadata SC(s) 820 and promotional data such as a graphic image file of the store's logo and a URL to the store's web site. An Offer SC(s) 841 template in the Metadata SC(s) 820 indicates which information can be overridden by the Electronic Digital Content Store(s) 103 in the Offer SC(s) 841 and what, if any, additional information is required by the Electronic Digital Content Store(s) 103 and what parts are retained in the embedded Metadata SC(s) 820.

[0111] Offer SC(s) 841 are included in a Transaction SC(s) 840 when an End-User(s) decides to purchase Content 113 from an Electronic Digital Content Store(s) 103. The Electronic Digital Content Store(s) 103 builds a Transaction SC(s) 840 and includes Offer SC(s) 841 for each Content 113 item being purchased and transmits it to the End-User Device(s) 109. The End-User Device(s) 109 receives the Transaction SC(s) 840 and validates the integrity of the Transaction SC(s) 840 and the included Offer SC(s) 841.

[0112] An Order SC(s) 850 is built by the End-User Device(s) 109 for each Content 113 item being purchased. Information is included from the Offer SC(s) 841, from the Transaction SC(s) 840, and from the configuration files of the End-User Device(s) 109. Order SC(s) 850 are sent to the Clearinghouse(s) 105 one at a time. The Clearinghouse

[0113] The Clearinghouse(s) 105 uses **Metadata** and **processes** Order SC(s) 850 to provide the End-User Device(s) 109 with everything that is required to a License Watermark 827 and increase purchased Content 113. One of the functions of the Clearinghouse(s) 105 is to decrypt the Symmetric Key 823 that are needed to decrypt the watermarking instructions from the Offer SC(s) 841 and the Content 113 from the Content SC(s) 830. An encrypted Symmetric Key 823 record actually contains more than the actual encrypted Symmetric Key 823. Before executing the encryption, the Content Provider(s) 101 may optionally append its name to the actual Symmetric Key 823 provides security against a plain Content Provider(s) 101 that has built its own Metadata SC(s) 820 and Content SC(s) 830 from legal SC(s). The Clearinghouse(s) 105 verifies that the name of the Content Provider(s) 101 is encrypted together with the Symmetric Key 823 matches the name of the Content Provider(s) 101 in the SC(s) certificate.

[0114] If there are any changes required to be made to the watermarking instructions by the Clearinghouse(s) 105, then the Clearinghouse(s) 105 decryps the Symmetric Key 823 and then modifies the watermarking instructions and encrypts them again using a new Symmetric Key 823. The Symmetric Key 823 is then re-encrypted using the Public Key 861 or the End-User Device(s) 109. The Clearinghouse(s) 105 also decryps the other Symmetric Key 823 in the SC(s) and encrypts them again with the Public Key 851 or the End-User Device(s) 109. The Clearinghouse(s) 105 builds a License SC(s) 860 that includes the newly encrypted Symmetric Key 823 and updated watermarking instructions and sends it to the End-User Device(s) 109 in response to the Order SC(s) 850. If the processing of the Order SC(s) 850 does not complete successfully, then the Clearinghouse(s) 105 returns to the End-User Device(s) 109 an HTML page or equivalent reporting the failure of the authentication process.

[0115] A License SC(s) 860 provides an End-User Device(s) 109 with everything that is needed to access a Content 113. Content SC(s) 850 are built by Content Provider(s) 101 and include encrypted Content 113 and metadata parts. The End-User Player Application 105 uses the Symmetric Key 823 from the License SC(s) 860 to decrypt the Content 113, metadata, and watermarking instructions. The watermarking instructions are then ethred into the Content 113 and the Content 113 is assembled and stored on the End-User Device(s) 109.

D. Metadata Secure Container 820 Format

[0116] The following table shows the parts that are included in a Metadata SC(s) 820. Each box in the Parts column is a separate object included in the SC(s) along with the BOM (with the exception of part names that are surrounded by [] characters). The BOM contains a record for each part included in the SC(s). The Part Exists column indicates whether the part itself is actually included in the SC(s) and the Digest column indicates whether a message digest is computed for the part. Some parts may not be propagated when a SC(s) is included in other SC(s) (as determined by the associated template), although the entire original BOM is propagated. This is done because the entire BOM is required by the Clearinghouse(s) 105 to verify the digital signature in the original SC(s).

[0117] The Key Description Part columns of the following table define information about the encryption key and algorithm part of the SC(s). Records in the Key Description part define information about the encryption key and algorithms that were used to encrypt parts within the SC(s) or parts within another SC(s). Each record indicates the Name column defines the name that is assigned to the part after it is decrypted. The Encrypt Alg column defines the encryption algorithm that was used to encrypt the part. The Key Id/Enc Key column defines either an identification of the encryption key that was used to encrypt the part or a base64 encoding of the encrypted part. The Digest column defines the encryption key that was used to encrypt the part. The Sym Key Alg is an optional parameter that defines the Symmetric Key 823 bit string that was used to encrypt the Symmetric Key 823 when the previous column is an encrypted Symmetric Key 822. The Sym Key Id column is an identification of the encryption key that was used to encrypt the Symmetric Key 823 when the Key Id/Enc Key column is an encrypted Symmetric Key 823.

[Content URL] - A parameter in a record in the Key Description part. This is a URL that points to the encrypted Content 113 in the Content (SIC) 650 that is associated with the Metadata (SIC) 620. The Metadata (SIC) 620 itself does not contain the encrypted Content 113.

[Metadata URL] - A parameter in a record in the Key Description part. This is a URL that points to the encrypted metadata in the Content (SIC) 350 that is associated with the Metadata (SIC) 620. The Metadata (SIC) 620 itself does not contain the encrypted metadata.

Content ID - A part that defines a unique ID assigned to a Content 113 item. There is more than one Content ID included in this part if the Metadata (SIC) 620 references more than one Content 113 item.

Metadata - Parts that contain information related to a Content 113 item such as the artist name and CD cover art in the case of a song. There may be multiple metadata parts, some of which may be encrypted. The internal structure of the metadata parts is dependent on the type of metadata contained therein.

Usage Conditions - A part that contains information that describes usage options, rules, and restrictions to be imposed on an End-User(s) for use of the Content 113.

Template(s) - Parts that define templates that describe the required and optional information for building the Watermarking Instructions. A part that contains the encrypted instructions and parameters for implementing watermarking in the Content 113. The watermarking instructions may be modified by the Clearinghouse(s) 105 and returned back to the End-User Device(s) 109 within the License (SIC) 660. There is a record in the Key Description

part that defines the encryption algorithm that was used to encrypt the watermarking instructions, the output part name to use when the watermarking instructions are decrypted, a base64 encoding of the encrypted Symmetric Key 623 till using that it was used to encrypt the watermarking instructions, the encryption algorithm that was used to encrypt the Symmetric Key 623, and the identification of the public key that is required to decrypt the Symmetric Key 623.

5
not occur using user name used to encrypt the workstation's public key that was used to encrypt the Symmetric Key 823, and the identification of the public key that is required to decrypt the Symmetric Key 823.

Clearinghouse(s) Certificate(s): A certificate from a certification authority or from the Clearinghouse(s) 105 that contains the signed Public Key 821 of the Clearinghouse(s) 105. There may be more than one certificate. In which case a hierarchical level structure is used with the highest level certificate containing the public key to open the next lowest level certificate is reached which contains the Public Key 821 of the Clearinghouse(s) 105.

Public Key 621 of the entity that created the SC(e). There may be more than one certificate, in which case a hierarchical level structure is used with the highest level certificate containing the public key to open the next level certificate, and so on, until the lowest level certificate is reached which contains the public key of the SC(e) creator. SC Version - A version number assigned to the SC(e) by the SC Packer Tool. SC ID - A unique ID assigned to the SC(e) by the entity that created the SC(e). SC Type - indicates the type of SC(e) (e.g. Metadata, Offer, Order, etc.)

Clearinghouse(s) URL - Address of the Clearinghouse(s) 105 that the End-User Player Application 195 should interact with to obtain the proper authorization to access the Content 113.

- This encrypted value is the digital signature.
- The Signature - A digest of the concatenated part digests encrypted with the public key of the entity that created the CTR.

- RSA and RCF - Default encryption algorithms used to encrypt the Symmetric Keys 8232 and data parts.
- Enc Sym Key - A base64 encoding of an encrypted key blob that, when decrypted, is used to decrypt a SCEs part.
- Enc Data - A base64 encoding of an encrypted data blob that, when decrypted, is used to decrypt a SCEs part.

E. Offer Secure Container 641 Format

some of the metadata parts, and BOM from the Metadata SC(s) 820 are also included in the Offer SC(s) 841.

65 [0120] The following describe the terms that are used in the above Offer SCI(e) 841 that were not previously de-
66 scribed for another SCI(e):

Metadata SC(0) BOM - The BOM from the original Metadata SC(0) 820. The record in the Offer SC(0) 841 BOM

26

28

Includes the digest of the Metadata SC(e) 620 BOM.

Additional and Overidden Fields - Usage conditions information that was overridden by the Electronic Digital Content Store(e) 103. This information is validated by the Clearinghouse(e) 105, by means of the modified SC(e) 5 template, to make sure that anything that the Electronic Digital Content Store(e) 103 overides is within the scope of its authorization.

Electronic Digital Content Store(e) Certificate - A certificate provided to the Electronic Digital Content Store(e) 103 by the Clearinghouse(e) 105 using its private key. This certificate is used by the End-User Player Application 105 to verify that the Electronic Digital Content Store(e) 103 is a valid distributor of Content 113. The End-User Player Application 105 and Clearinghouse(e) 105 can verify that the Electronic Digital Content Store(e) 103 is an authorized distributor by decrypting the certificate's signature with the Clearinghouse(e) 105 Public Key 621. The End-User Player Application 105 keeps a local copy of the Clearinghouse(e) 105 Public Key 621 that it receives as part of its initialization during installation.

F. Transaction Secure Container 640 Format

[0123] The following table shows the parts that are included in the Transaction SC(e) 640 as well as its BOM and Key Description parts.

Part	Part Type	Value	Usage	Value	Usage	Part Name	Content Type	Content Description	Content ID	Content Version
20	SC Version									
21	SC ID									
22	SC Type									
23	SC Publisher									
24	SC									
25	SC									
26	SC									
27	SC									
28	SC									
29	SC									
30	SC									
31	SC									
32	SC									
33	SC									
34	SC									
35	SC									
36	SC									
37	SC									
38	SC									
39	SC									
40	SC									
41	SC									
42	SC									
43	SC									
44	SC									
45	SC									
46	SC									
47	SC									
48	SC									
49	SC									
50	SC									
51	SC									
52	SC									
53	SC									
54	SC									
55	SC									
56	SC									
57	SC									
58	SC									
59	SC									
60	SC									

the Symmetric Key 623. The End-User(e) Public Key 681 is transmitted to the Electronic Digital Content Store

(e) 103 during the purchase transaction.

Offer SC(e) - Offer SC(e) 641 for the Content 113 items that were purchased.

Selection of Content Use - An array of Usage Conditions for each Content 113 item being purchased by the End-User(e). There is an entry for each Offer SC(e) 641.

HTML to Display - One or more HTML pages that the End-User Player Application 105 displays in the Internet browser window upon receipt of the Transaction SC(e) 640 or during the interaction between the End-User Device (e) 109 and the Clearinghouse(e) 105.

[0123] When the End-User Device(e) 109 receives a Transaction SC(e) 640, the following steps may be performed to verify the integrity and authenticity of the SC(e):

1. Verify the integrity of the Electronic Digital Content Store(e) 103 certificate using the Public Key 621 of the Clearinghouse(e) 105. The Public Key 621 of the Clearinghouse(e) 105 was stored at the End-User Device(e) 109 after it was received as part of the initialization of the End-User Player Application 105 during its installation process.
2. Verify the Digital Signature 643 of the SC(e) using the public key from the Electronic Digital Content Store(e) 103 certificate.
3. Verify the hashes of the SC(e) parts.
4. Verify the integrity and authenticity of each Offer SC(e) 641 included in the Transaction SC(e) 640.

G. Order Secure Container 650 Format

[0124] The following table shows the parts that are included in the Order SC(e) 650 as well as its BOM and Key Description parts. These parts either provide information to the Clearinghouse(e) 105 for decryption and verification purposes or is validated by the Clearinghouse(e) 105. The parts and BOM from the Offer SC(e) 641 are also included in the Order SC(e) 650. The same steps in the Part Exists column of the Metadata SC(e) BOM indicate that the some of those parts are not included in the Order SC(e) 650. The BOM from the Metadata SC(e) 620 is also included without any change so that the Clearinghouse(e) 105 can validate the integrity of the Metadata SC(e) 620 and its parts.

Part	Part Type	Value	Usage	Value	Usage	Part Name	Content Type	Content Description	Content ID	Content Version
61	SC Version									
62	SC ID									
63	SC Type									
64	SC Publisher									
65	SC									
66	SC									
67	SC									
68	SC									
69	SC									
70	SC									
71	SC									
72	SC									
73	SC									
74	SC									
75	SC									
76	SC									
77	SC									
78	SC									
79	SC									
80	SC									
81	SC									
82	SC									
83	SC									
84	SC									
85	SC									
86	SC									
87	SC									
88	SC									
89	SC									
90	SC									
91	SC									
92	SC									
93	SC									
94	SC									
95	SC									
96	SC									
97	SC									
98	SC									
99	SC									
100	SC									
101	SC									
102	SC									
103	SC									
104	SC									
105	SC									
106	SC									
107	SC									
108	SC									
109	SC									
110	SC									
111	SC									
112	SC									
113	SC									
114	SC									
115	SC									
116	SC									
117	SC									
118	SC									
119	SC									
120	SC									
121	SC									
122	SC									
123	SC									
124	SC									
125	SC									
126	SC									
127	SC									
128	SC									
129	SC									
130	SC									
131	SC									
132	SC									
133	SC									
134	SC									
135	SC									
136	SC									
137	SC									
138	SC									
139	SC									
140	SC									
141	SC									
142	SC									
143	SC									
144	SC									
145	SC									
146	SC									
147	SC									
148	SC									
149	SC									
150	SC									
151	SC									
152	SC									
153	SC									
154	SC									
155	SC									
156	SC									
157	SC									
158	SC									
159	SC									
160	SC									
161	SC									
162	SC									
163	SC									
164	SC									
165	SC									
166	SC									
167	SC									
168	SC									
169	SC									
170	SC									
171	SC									
172	SC									
173	SC									
174	SC									
175	SC									
176	SC									
177	SC									
178	SC									
179	SC									
180	SC									
181	SC									
182	SC									
183	SC									
184	SC									
185	SC									
186	SC									
187	SC									
188	SC									
189	SC									
190	SC									

that created the Offer SC(s) 641 does not handle the customer billing, in which case the Clearinghouse(s) 105 may handle the billing.

H. License Secure Container 680 Format

[0126] The following table shows the parts that are included in the License SC(s) 680 as well as its BOM. As shown in the Key Description part, the Symmetric Keys 623 that are required for decrypting the watermarking instructions, Content 113, and Content 113 metadata have been re-encrypted by the Clearinghouse(s) 105 using the End-User(s) "Public Key 681. When the End-User Device(s) 109 receives the License SC(s) 680 it decrypts the Symmetric Keys 623 and uses them to access the encrypted parts from the License SC(s) 680 and the Content SC(s) 630.

Part	Part Exist	BOM	Digest
15	[Content URL]		
16	[Metadata URL]		
17	SC(s) Version		
18	SC(s) ID		
19	SC(s) Type		
20	SC(s) Publisher		
21	Date		
22	Expiration Date		
23	Digital Algorithm ID		
24	Digital Signature		
25	DigSig ID		
26	Content ID		
27	Order SC(s) ID		
28	Watermarking Instructions		
29	Key Description Part		
30	Certificate(s)		
31	Digital Signature		

Content ID	Output Part	Key Sym Key	Key	EU Pub Key
32	Encrypted Content	Yes	Yes	
33	Encrypted Metadata	Yes	Yes	
34	Metadata	Yes	Yes	
35	Certificate(s)	Yes	No	
36	Digital Signature			

[0127] The following describes the terms that are used in the above License SC(s) 680 that were not previously described for another SC(s):

- EU Pub Key - An Identifier that indicates that the End-User(s)' Public Key 681 was used to encrypt the data.
- Order SC(s) ID - The SC(s) ID taken from the Order SC(s) 680 BOM.
- Certificate Revocation List - An optional list of certificate IDs which were previously issued and signed by the Clearinghouse(s) 105, but are no longer considered to be valid. Any SC(s) that have a signature which can be verified by a certificate that is included in the revocation list are invalid SC(s). The End-User Player Application 185 stores a copy of the Clearinghouse's 105 certificate revocation list on the End-User Device(s) 109. Whenever a revocation list is received, the End-User Player Application 185 replaces its local copy if the new one is more up to date. Revocation lists includes a version number or a timestamp (or both) in order to determine which list is the most recent.

[0127] The following describes the terms that are used in the above Content SC(s) 630 that were not previously described for another SC(s):

- Encrypted Content - Content 113 that was encrypted by a Content Provider(s) 101 using a Symmetric Key 623.
- Encrypted Metadata - Metadata associated with the Content 113 that was encrypted by a Content Provider(s) 101 using a Symmetric Key 623.
- [0130] There is no Key Description part included in the Content SC(s) 630 since the keys required to decrypt the encrypted parts are in the License SC(s) 680 that is built at the Clearinghouse(s) 105.

VI. SECURE CONTAINER PACKING AND UNPACKING

A. Overview

- [0131] The SC(s) Packer is a 32-bit Windows® program with an API (Application Programming Interface) that can be called in either a multiple or single step process to create a SC(s) with all of the specified parts. The SC(s) Packer 151, 152, 153 variety of hardware platforms supporting Windows® program at the Content Provider(s) 101, Clearinghouse(s) 105, Electronic Digital Content Store(s) 103 and other sites requiring SC(s) Packing. A BOM and, if necessary, a Key Description part are created and included in the SC(s). A set of packer APIs allow the caller to specify the information required to generate the records in the BOM and Key Description parts and to include parts in the SC(s). Encryption of parts and Symmetric Keys 623 as well as computing the digests and the digital signature is also be performed by the packer. Encryption and digest algorithms that are supported by the packer are included in the packer code or they are called through an external interface.
- [0132] The interface to the packer for building a SC(s) is done by an API that accepts the following parameters as input:

I. Content Secure Container Format

[0128] The following table shows the parts that are included in the Content SC(s) 630 as well as the BOM:

Part Exist	BOM	Digest
SC(s) Version		
SC(s) ID		
SC(s) Type		
SC(s) Publisher		
Clearinghouse(s) URL		
Expiration Date		
Digital Algorithm ID		
Digital Signature		

- A pointer to a buffer of concatenated structures. Each structure in the buffer is a command to the packer with the information that is required to execute the command. Packer commands include adding a part to the SC(e) with an associated BOM record, adding a record to the BOM, and adding records to the Key Description part.
- A value indicating the size of concatenated structures contained in the above described buffer.
- Name and location of the BOM part.
- A value with each bit being a defined flag or a reserved flag for future use. The following flags are currently defined:

[0133] In an alternate embodiment, the interface to the packer for building a SC(e) is done by APIs that accept the following parameters as input:

- First, an API is called to create a Bill of Materials (BOM) part by passing in pointer to a structure that consists of information that is used to initialize SC(e) settings that are denoted as IP records in the SC(e) BOM part, the last step that is performed when building a SC(e).
- Indication as to whether the digital signature is omitted from the BOM part. If this flag is not set, then the digital signature is computed right before the SC(e) is bundled into a single object.

- [0133] In an alternate embodiment, the interface to the packer for building a SC(e) is done by APIs that accept the following flags are currently defined:
- Indication as to whether all of the parts of the SC(e) should be bundled together into a single file after all of the structures in the buffer have been processed. Bundling the parts into a single object is the last step that is performed when building a SC(e).
- A value indicating the size of concatenated structures contained in the above described buffer.
- A value with each bit being a defined flag or a reserved flag for future use. The following flags are currently defined:

[0133] In an alternate embodiment, the interface to the packer for building a SC(e) is done by APIs that accept the following flags are currently defined:

- The structure in the buffer have been processed. Bundling the parts into a single object is the last step that is performed when building a SC(e).
- Indication as to whether the digital signature is omitted from the BOM part. If this flag is not set, then the digital signature is computed right before the SC(e) is bundled into a single object.

- [0133] In an alternate embodiment, the interface to the packer for building a SC(e) is done by APIs that accept the following flags are currently defined:
- The structure in the buffer have been processed. Bundling the parts into a single object is the last step that is performed when building a SC(e).
- Indication as to whether the digital signature is omitted from the BOM part. If this flag is not set, then the digital signature is computed right before the SC(e) is bundled into a single object.

[0133] In an alternate embodiment, the interface to the packer for building a SC(e) is done by APIs that accept the following flags are currently defined:

- The structure in the buffer have been processed. Bundling the parts into a single object is the last step that is performed when building a SC(e).
- Indication as to whether the digital signature is omitted from the BOM part. If this flag is not set, then the digital signature is computed right before the SC(e) is bundled into a single object.

[0133] In an alternate embodiment, the interface to the packer for building a SC(e) is done by APIs that accept the following flags are currently defined:

- The structure in the buffer have been processed. Bundling the parts into a single object is the last step that is performed when building a SC(e).
- Indication as to whether the digital signature is omitted from the BOM part. If this flag is not set, then the digital signature is computed right before the SC(e) is bundled into a single object.

[0133] In an alternate embodiment, the interface to the packer for building a SC(e) is done by APIs that accept the following flags are currently defined:

- The structure in the buffer have been processed. Bundling the parts into a single object is the last step that is performed when building a SC(e).
- Indication as to whether the digital signature is omitted from the BOM part. If this flag is not set, then the digital signature is computed right before the SC(e) is bundled into a single object.

[0133] In an alternate embodiment, the interface to the packer for building a SC(e) is done by APIs that accept the following flags are currently defined:

- The structure in the buffer have been processed. Bundling the parts into a single object is the last step that is performed when building a SC(e).
- Indication as to whether the digital signature is omitted from the BOM part. If this flag is not set, then the digital signature is computed right before the SC(e) is bundled into a single object.

[0133] In an alternate embodiment, the interface to the packer for building a SC(e) is done by APIs that accept the following flags are currently defined:

- The structure in the buffer have been processed. Bundling the parts into a single object is the last step that is performed when building a SC(e).
- Indication as to whether the digital signature is omitted from the BOM part. If this flag is not set, then the digital signature is computed right before the SC(e) is bundled into a single object.

[0133] In an alternate embodiment, the interface to the packer for building a SC(e) is done by APIs that accept the following flags are currently defined:

- The structure in the buffer have been processed. Bundling the parts into a single object is the last step that is performed when building a SC(e).
- Indication as to whether the digital signature is omitted from the BOM part. If this flag is not set, then the digital signature is computed right before the SC(e) is bundled into a single object.

[0133] In an alternate embodiment, the interface to the packer for building a SC(e) is done by APIs that accept the following flags are currently defined:

- The structure in the buffer have been processed. Bundling the parts into a single object is the last step that is performed when building a SC(e).
- Indication as to whether the digital signature is omitted from the BOM part. If this flag is not set, then the digital signature is computed right before the SC(e) is bundled into a single object.

- ORD - An Order SC(e) 650.
- OFF - An Offer SC(e) 641.
- LIC - A License SC(e).
- TRA - A Transaction SC(e) 640.
- MET - A Metadata SC(e) 620.
- CON - A Content SC(e) 630.

6 A value

- The A property identifies the author or publisher of the SC(e). Author/publisher Identifies should be unambiguous and/or registered with the Clearinghouse(s) 105.

10 D value

- The D property identifies the date, and optionally, the time that the SC(e) was created. The value should be of the form `yyymmd[ff@hhmm[ss][.ff]]` representing year/month/day@hour:min:sec-on decimal-fraction-4-second (time-zone). Optional parts of the value are enclosed in [] characters.

14 E value

- The E property identifies the date, and optionally, the time that the SC(e) expires. The value should be the same form used in the D property that was previously defined. The expiration date/time should be compared, whenever possible, with the date/time at the Clearinghouse(s) 105.

20 F value

- The CCURL property identifies the URL of the Clearinghouse(s) 105. The value should be of the form of a valid external URL.

24 G value

- The H property identifies the algorithm that was used to calculate the message digests for the parts included in the SC(e). An example digest algorithm is MD5.

28 H value

- A D record is a data or part entry record that contains information that identifies the type of part, the name of the part, the (optional) digest of the part, and an (optional) indication that the part is not included in the SC(e). The A - sign immediately after the type identifier is used to indicate that the part is not included in the SC(e). The following are reserved types of data or part records:

32 K part_name [digest]

- Specifies the Key Description part.

33 W part_name [digest]

- Specifies the watermarking Instructions part.

35 C part_name [digest]

- Specifies the certificate(s) used to validate the digital signature.

40 T part_name [digest]

- Specifies the Usage Conditions part.

41 YF part_name [digest]

- Specifies the Template part for the Offer SC(e) 641.

42 YO part_name [digest]

- Specifies the Template part for the Order SC(e) 650.

43 YL part_name [digest]

- Specifies the Template part for the License SC(e) 680.

45 ID part_name [digest]

- Specifies the ID(s) of the Content 113 of the Item(s) of Content 113 being referenced.

46 CH part_name [digest]

- Specifies the Clearinghouse(s) 105 certificate part.

47 SP part_name [digest]

- Specifies the Electronic Digital Content Store(s) 103 certificate part.

48 B part_name [digest]

- Specifies a BOM part for another SC(e) that has its parts or a subset of its parts included in this SC(e).

49 BP part_name sc_part_name [digest]

- Specifies a BOM part for another SC(e) that is included as a single part in the SC(e). The sc_part_name parameter is the name of the SC(e) part that is included in this SC(e) and that this BOM part defines. A BOM that is identical to the one is also included in the SC(e) that is defined by the sc_part_name parameter.

50 D part_name [digest]

- The T property specifies the type of the SC(e), which should be one of:

Specifies a data (or metadata) part.

5 An S record is a signature record that is used to define the digital signature of the SC(s). The digital signature
is specified as follows:

6 8 key_identifier signature_string signature_algorithm

7 The S record contains the key_identifier to indicate the encryption key of the signature, the signature_string,
which is the base64 encoding of the digital signature bitstring, and the signature algorithm that was used to
encrypt the digest to create the digital signature.

10 C. Key Description Part

11 [0137] The Key Description part is created by the provider to provide information about encryption keys that are needed
for decryption of SC(s) encrypted parts. The encrypted parts may be included in the SC(s) being built, or may be in
other SC(s) which are referred to by the SC(s) being built. The Key Description part is a text file that contains records
of information about the encryption keys and the parts for which the encryption keys are used. Each record in the Key
Description part is on a single line with a new line indicating the start of a new record.

12 [0138] The following record type is used within a Key Description part and is defined as follows:

13 K encrypted_part_name result_part_name key encryption_algorithm identifier public_key_identifier
key encryption_algorithm identifier public_key_identifier

14 A K record specifies an encrypted part that may be included in this SC(s) or may be included in another SC.
(b) that is referred to by this record. The encrypted_part_name is either the name of part in this SC(s) or a URL
pointing to the name of the encrypted part in another SC(s). The result_part_name is the name that is given to the
decrypted part. The part encryption_algorithm identifier indicates the encryption algorithm that was used to en-
crypt the part. The public_key_identifier is an identifier of the key that was used to encrypt the Symmetric Key 823.

15 The key encryption algorithm identifier indicates the encryption algorithm that was used to encrypt the Sym-
metric Key 823. The encrypted_symmetric_key is a base64 encoding of the encrypted Symmetric Key 823 URL string
that was used to encrypt the part.

20 VII. CLEARINGHOUSE(s) 103

21 A. Overview

22 [0139] The Clearinghouse(s) 103 is responsible for the rights management functions of the Secure Digital Content
System 103, verification of rights to Content 113, integrity and authenticity validation of the buying transaction and
related information, distribution of Content encryption keys or Symmetric Keys 823 to End-User Device(s) 109, tracking
the distribution of those keys, and reporting or transaction summaries to Electronic Digital Content Store(s) 103 and
Content Provider(s) 101. Content encryption keys are used by End-User Device(s) 109 to unlock Content 113 for which
they have obtained rights, typically by a purchase transaction from an authorized Electronic Digital Content Store(s)
103. Before a Content encryption key is sent to an End-User Device(s) 109, the Clearinghouse(s) 103 goes through
a verification process to validate the authenticity of the entity that is selling the Content 113 and the rights that the End-
User Device(s) 109 has to the Content 113. This is called the SC Analysis Tool 105. In some configurations the Clear-
inghouse(s) 103 may also handle the financial settlement of Content 113 purchases by co-operating with a system at the
Clearinghouse(s) 105 that performs the Electronic Digital Content Store(s) 103 functions of credit card authorization
and billing. The Clearinghouse(s) 105 uses OEM packages such as iCommerce and Taxware to handle the credit card
processing and local sales taxes.

23 Electronic Digital Content Store(s) Embodiment

30 [0140] An Electronic Digital Content Store(s) 103 that wants to participate as a seller of Content 113 in the Secure
Digital Content Electronic Distribution System 100 makes a request to one or more of the Digital Content Provider(s)
40 for making the request as long as the two parties come to an agreement. After the digital content label such
as a Music Label e.g. Sony, Time-Warner, etc. decides to allow the Electronic Digital Content Store(s) 103 to sell its
Content 113, the Clearinghouse(s) 105 is contacted, usually via Email, with a request that the Electronic Digital Content
Store(s) 103 be added to the Secure Digital Content Electronic Distribution System 100. The digital content label
provides the name of the Electronic Digital Content Store(s) 103 and any other information that may be required for

the Clearinghouse(s) 105 to create a digital certificate for the Electronic Digital Content Store(s) 103. The digital cer-
tificate is sent to the digital content label, and then forwarded by the digital content label to the
Electronic Digital Content Store(s) 103. The Clearinghouse(s) 105 maintains a database of digital certificates that it
has assigned. Each certificate includes a version number, a unique serial number, the signing algorithm, the name of
the issuer (e.g., the name of Clearinghouse(s) 105), range of dates for which the certificate is considered to be valid,
the name Electronic Digital Content Store(s) 103, the public key of the Electronic Digital Content Store(s) 103, and a
hash code of all of the other information signed using the private key of the Clearinghouse(s) 105. Entities that have
the Public Key 821 of the Clearinghouse(s) 105 can validate the certificate and then be assured that a SC(s) with a
signature that can be validated using the public key from the certificate is a valid SC(s).

45 [0141] After the Electronic Digital Content Store(s) 103 has received its digital certificate that was created by the
Clearinghouse(s) 105 and the necessary tools for processing the SC(s) from the digital content label, it can begin
offering Content 113 that can be purchased by End-User(s). The Electronic Digital Content Store(s) 103 includes its
certificates and the Transaction SC(s) 640 and signs the SC(s) using its Digital Signature 643. The End-User Device
50 (b) 109 verifies that the Electronic Digital Content Store(s) 103 is valid by its Digital Signature 643. The End-User Device(s)
109 checks the digital certificate revocation list maintained by the Clearinghouse(s) 105. The revocation list
may be included as one of the parts in a license SC(s) 660 that is created by the Clearinghouse(s) 105. End-User Device(s)
109 keeps a copy of the revocation list on the End-User Device(s) 109 so they can use it as part of the SC(s).
Device(s) 109 determines whether a new revocation list is included and if so, the local revocation list on the
License SC(s) 660 is updated.

55 B. Rights Management Processing

60 Order SC(s) Analysis

65 [0142] The Clearinghouse(s) 105 receives an Order SC(s) 650 from an End-User(s) after the End-User(s) has
66 received the Transaction SC(s) 640, which include the Order SC(s) 650 from the Electronic Digital Content Store(s) 103.
67 The Order SC(s) 650 consists of parts that contain information relative to the Content 113 and its use. Information
68 about the Electronic Digital Content Store(s) 103 that is selling the Content 113, and information about the End-User
69 (b) that is purchasing the Content 113. Before the Clearinghouse(s) 105 begins processing the information in the Order
70 SC(s) 650, it first performs some processing to insure that the SC(s) is in fact valid and the data it contains has not
71 been corrupted in any way.

75 Validation

76 [0143] The Clearinghouse(s) 105 begins the validation of Order SC(s) 650 by verifying the digital signatures, then
the Clearinghouse(s) 105 deciphers the Content 113 of the signature of the Order SC(s) 650 parts. To validate the digital signatures, first the
Clearinghouse(s) 105 deciphers the Content 113 of the signature of the Order SC(s) 650 parts. To validate the digital signatures, first the
Clearinghouse(s) 105 (the signing entity could be the Content Provider(s) 101, the Electronic Digital Content Store(s) 103,
40 included if signed. (The signing entity could be the Content Provider(s) 101, the Electronic Digital Content Store(s) 103,
103, the End-User Device(s) 109 or any combination of them.) Then, the Clearinghouse(s) 105 calculates the digest
of the concatenated part digests of the SC(s) and compares it with the digital signature's decrypted Content 113. If the
two values match, the digital signature is valid. To verify the integrity of each part, the Clearinghouse(s) 105 compares
45 the digest of the part and compares it to the digest value in the SC(s). The Clearinghouse(s) 105 follows the same
process to verify the digital signatures and part integrity for the Metadata and Offer SC(s) 661 parts included within
the Order SC(s) 650.

50 [0144] The process of verification of the Transaction and Offer SC(s) 640 digital signatures also indirectly verifies
that the Electronic Digital Content Store(s) 103 is authorized by the Secure Digital Content Electronic Distribution
System 100. This is based on the fact that the Clearinghouse(s) 105 is the issuer of the certificate. Alternatively, the
Clearinghouse(s) 105 would be able to successfully verify the digital signatures of the Transaction SC(s) 640 and Offer
SC(s) 661 using the public key from the Electronic Digital Content Store(s) 103, but only if the entity signing the SC(s)
55 has ownership of the associated private key. Only the Electronic Digital Content Store(s) 103 has ownership of the
Content Key. Notice that, the Clearinghouse(s) 105 does not need to have a local database of the Electronic Digital
Content Store(s) 103. Since the store uses the Clearinghouse Public Key to sign the Transaction SC(s) 640 Offer SC(s)
60 641 public key.

56 [0145] Then, the Store Usage Conditions 519 of the Content 113 which the End-User(s) is purchasing are validated
by the Clearinghouse(s) 105 to insure that they fall within the restrictions that were set in the Metadata SC(s) 620.

Recall that the Metadata SCI(6) 820 is included within the Order SCI(4) 850.

Key Processing

6

[0146] Processing of the encrypted Symmetric Keys 823 and of the watermarking instructions are done by the Clearinghouse(s) 105 after authentication and the integrity check of the Order SCI(4) 850, the validation of the Electronic Digital Content Store(s) 103 and the validation of the Store Usage Conditions 519 have been completed successfully. The Metadata SCI(6) 820 portion of the Order SCI(4) 850 typically has several Symmetric Keys 823 located in the Key Description part that were encrypted using the Public Key 922 of the Clearinghouse(s) 105. Encryption of the Symmetric Keys 823 are done by the Content Provider(s) 101 when the Metadata SCI(6) 820 was created.

[0147] One Symmetric Key 823 are used for describing the watermarking instructions and the others for describing the Content 113 and any encrypted metadata. Since Content 113 can represent a single song or an entire album of songs on a CD, a different Symmetric Key 823 may be used for each song. The watermarking instructions are included within the Metadata SCI(6) 820 portion in the Order SCI(4) 850. The Content 113 and encrypted metadata are in the Content SCI(6) 830 at a Content Hosting Site(s) 111. The URL and part names of the encrypted Content 113 and metadata parts, within the Content SCI(6) 830, are included in the Key Description part of the Metadata SCI(6) 820 portion of the Order SCI(4) 850. The Clearinghouse(s) 105 uses its private key to decrypt the Symmetric Keys 823 and then encrypts each of them using the Public Key 961 of the End-User Device(s) 109. The Public Key 961 of the End-User Device(s) 109 is retrieved from the Order SCI(4) 850. The new encrypted Symmetric Keys 823 are included in the Key Description part of the License SCI(4) 860 that the Clearinghouse(s) 105 returns to the End-User Device(s) 109.

[0148] During the time of processing the Symmetric Keys 823, the Clearinghouse(s) 105 may want to make modifications to the watermarking instructions. If this is the case, then after the Clearinghouse(s) 105 decrypts the Symmetric Keys 823, the watermarking instructions are modified and re-encrypted. The new watermarking instructions are included as one of the parts within the License SCI(4) 860 that is returned to the End-User Device(s) 109.

[0149] If all of the processing of the Order SCI(4) 850 is successful, then the Clearinghouse(s) 105 returns a License SCI(4) 860 to the End-User Device(s) 109. The End-User Device(s) 109 uses the License SCI(4) 860 information to download the Content SCI(6) 830 and access the encrypted Content 113 and metadata. The watermarking instructions are also executed by the End-User Device(s) 109.

[0150] If the Clearinghouse(s) 105 is not able to successfully process the Order SCI(4) 850, then an HTML page is returned to the End-User Device(s) 109 and displayed in an Internet browser window. The HTML page indicates the reason that the Clearinghouse(s) 105 was unable to process the transaction.

[0151] In an alternate embodiment, if the user has purchased a copy of the Content 113 prior to the release date set for the sale, the License(s) 860 is returned without the Symmetric Keys 823. The License(s) 860 is returned to the Clearinghouse(s) 105 on or after the release date to receive the Symmetric Keys 823. As an example, the Content Provider(s) 101 allow users to download a new song prior to the release date for the song to enable customers to download the song and be prepared to play the song before a date set by the Content Provider(s) 101. This allows immediate opening of the Content 113 on the release date without having to content for bandwidth and download time on the release date.

C. Country Specific Parameters

4

[0152] Optionally, the Clearinghouse(s) 105 uses the domain name of the End-User Device(s) 109 and, whenever possible, the credit card billing address to determine the country location of the End-User(s). If there are any restrictions for the sale of Content 113 in the country where the End-User(s) resides, then the Clearinghouse(s) 105 insures that the transaction being processed is not violating any of those restrictions before transmitting License SCI(4) 860 to the End-User Device(s) 109. The Electronic Digital Content Store(s) 103 is also expected to participate in managing the distribution of Content 113 to various countries by performing the same checks as the Clearinghouse(s) 105. The Clearinghouse(s) 105 does whatever checking that it can in case the Electronic Digital Content Store(s) 103 is ignoring the country specific rules set by the Content Provider(s) 101.

D. Audit Logs and Tracking

6

[0153] The Clearinghouse(s) 105 maintains a Audit Logs 150 of information for each operation that is performed during Content 113 purchases, transactions and report request transactions. The information can be used for a variety of purposes such as audits of the Secure Digital Content Electronic Distribution System 100, generation of reports, and data mining.

[0154] The Clearinghouse(s) 105 also maintains account balances in Billing Subsystem 182 for the Electronic Digital Content Store(s) 103. Pricing structure for the Electronic Digital Content Store(s) 103 is provided to the Clearinghouse

(a) 105 by the digital content labels. This information can include things like current specials, volume discounts, and account deficit limits that need to be imposed on the Electronic Digital Content Store(s) 103. The Clearinghouse(s) 105 uses the pricing information to track the balances of the Electronic Digital Content Store(s) 103 and insure that they do not exceed their deficit limits set by the Content Provider(s) 101.

[0155] The following operations are typically logged by the Clearinghouse(s) 105:

- End-User Device(s) 109 requests for License SCI(4) 860

- Credit card authorization number when the Clearinghouse(s) 105 handles the billing

- Disposition of License SCI(4) 860 to End-User Device(s) 109

- Requests for reports

- Notification from the End-User(s) that the Content SCI(6) 830 and License SCI(4) 860 were received and validated

[0156] The following information is typically logged by the Clearinghouse(s) 105 for a License SCI(4) 860:

- End-User Device(s) 109 requests for License SCI(4) 860

- Date and time of the request

- Date and time of the purchase transaction

- Content ID of the item being purchased

- Identification of the Content Provider(s) 101

- Identification of the Credit Card 519

- Identification of the End-User Device(s) 109

- Identification of the Electronic Digital Content Store(s) 103

- Identification of the Electronic Digital Content Store(s) 103

- End-User(s) credit card information (if the Clearinghouse(s) 105 is handling the billing)

- Date and time of the request

- Amount charged to the credit card

- Content ID of the item being purchased

- Transaction ID 532 that was added by the Electronic Digital Content Store(s) 103

- Identification of the Electronic Digital Content Store(s) 103

- Identification of the End-User(s)

- End-User(s) credit card information

- Authorization number received from the clearer of the credit card

[0157] The following information is typically logged by the Clearinghouse(s) 105 for an End-User's credit card validation:

- Date and time of the request

- Content ID of the item being purchased

- Transaction ID 532 that was added by the Electronic Digital Content Store(s) 103

- Identification of the Electronic Digital Content Store(s) 103

- Identification of the End-User(s)

- End-User(s) credit card information

- Date and time of the request

- Content ID of the item being purchased

- Identification of Content Provider(s) 101

- Usage Conditions 517

- Type of report being requested

- Parameters used to generate the report

- Identifier of the entity requesting the report

[0158] The following information is typically logged when a report request is made:

- Date and time of the request

- Data and time the report was sent out

- Type of report being requested

- Parameters used to generate the report

- Identifier of the entity requesting the report

E. Reporting of Results

[0160] Reports are generated by the Clearinghouse(s) 105 using the information that the Clearinghouse(s) 105 logged during End-User(s) purchase transaction. Content Provider(s) 101 and Electronic Digital Content Store(s) 103 can request transaction reports from the Clearinghouse(s) 105 via a Payment Verification Interface 183 so they can reconcile their own transaction databases with the information logged by the Clearinghouse(s) 105. The Clearinghouse(s) 105 can also provide periodic reports to the Content Provider(s) 101 and Electronic Digital Content Store(s) 103.

[0161] The Clearinghouse(s) 105 defines a secure electronic interface which allows Content Provider(s) 101 and Electronic Digital Content Store(s) 103 to request and receive reports. The Report Request SC(s) 105 includes a certificate that was assigned by the Clearinghouse(s) 105 to the entity initiating the request. The Clearinghouse(s) 105 uses the certificate and the SC's digital signature to verify that the request originated from an authorized entity. The request also includes parameters, such as time duration, that define the scope of the report. The Clearinghouse(s) 105 validates the request parameters to insure that requesters can only receive information for which they are permitted to have.

[0162] If the Clearinghouse(s) 105 determines that the Report Request SC(s) is authentic and valid, then the Clearinghouse(s) 105 generates a report and pack it into a Report SC(s) to be sent to the entity that initiated the request. Some reports may be automatically generated at defined time intervals and stored at the Clearinghouse(s) 105 so they can be immediately sent when a request is received. The format of the data included in the report is defined in a later version of this document.

F. Billing and Payment Verification

[0163] Billing of Content 113 can be handled either by the Clearinghouse(s) 105 or by the Electronic Digital Content Store(s) 103. In the case where the Clearinghouse(s) 105 handles the billing of the electronic Content 113, the Electronic Digital Content Store(s) 103 separates the End-User(s)' order into electronic goods and, if applicable, physical goods. The Electronic Digital Content Store(s) 103 then, notifies the Clearinghouse(s) 105 of the transaction, including the End-User(s)' billing information, and the total amount that needs to be authorized. The Clearinghouse(s) 105 authorizes the End-User(s)' credit card and returns a notification back to the Electronic Digital Content Store(s) 103. At the same time the Clearinghouse(s) 105 is authorizing the End-User(s)' credit card, the Electronic Digital Content Store(s) 103 can charge the End-User(s)' credit card for any physical goods that are being purchased. After each electronic item is downloaded by the End-User Device(s) 109, the Clearinghouse(s) 105 is notified so the End-User(s)' credit card can be charged. This occurs as the last step by the End-User Device(s) 109 before the Content 113 is enabled for use at the End-User Device(s) 109.

[0164] In the case where the Electronic Digital Content Store(s) 103 handles the billing of the electronic Content 113, the Clearinghouse(s) 105 is not notified about the transaction until the End-User Device(s) 109 sends the Order SC (e) 850 to the Clearinghouse(s) 105. The Clearinghouse(s) 105 is still notified by the End-User Device(s) 109 after each electronic item is downloaded. When the Clearinghouse(s) 105 is notified it sends a notification to the Electronic Digital Content Store(s) 103 so that the Electronic Digital Content Store(s) 103 can charge the End-User(s)' credit card.

[0165] The Secure Digital Content Distribution System 100 provides the ability to handle retransmissions of Content 113. This is typically performed by a Customer Service Interface 184. Electronic Digital Content Store(s) 103 provides a user interface that the End-User(s) can step through in order to initiate a retransmission. The End-User(s) pose to the Electronic Digital Content Store(s) 103 site where the Content 113 item was purchased in order to request a retransmission of the Content 113.

[0166] Retransmissions of Content 113 are done when an End-User(s) requests a new copy of a previously purchased Content 113 item because the Content 113 could not be downloaded or the Content 113 that was downloaded is not useable. The Electronic Digital Content Store(s) 103 determines whether the End-User(s) is entitled to a retransmission of the Content 113. If the End-User(s) is entitled to a retransmission, then the Electronic Digital Content Store(s) 103 builds a Transaction SC(s) 840 that includes the Order SC(s) 841 of the Content 113 item(s) being retransmitted. The Transaction SC(s) 840 is sent to the End-User Device(s) 109 and the download stops as for a purchase transaction. The purchase is performed by the End-User(s). If the Content 113 item has an scrambled key(s) in the key library for the Content 113 item(s) undergoing retransmission, then the Transaction SC(s) 840 includes information that instructs the End-User Device(s) 109 to delete the scrambled key(s).

[0167] In the case where the Clearinghouse(s) 105 handles the financial settlement of Content 113 purchases, the Electronic Digital Content Store(s) 103 includes a tag in the Transaction SC(s) 840 that is carried forward to the Clearinghouse(s) 105 in the Order SC(s) 850. The Clearinghouse(s) 105 interprets the tag in the Order SC(s) 850 and proceeds with the transaction without charging the End-User(s) for the purchase of the Content 113.

VII. CONTENT PROVIDER

A. Overview

[0168] The Content Provider(s) 101 in the Secure Digital Content Electronic Distribution System 100 is the digital content label or the entity who owns the rights to the Content 113. The role of the Content Provider(s) 101 is to prepare the Content 113 for distribution and make information about the Content 113 available to Electronic Digital Content Store(s) 103 or retailers of the downloadable electronic versions of the Content 113. To provide the utmost security and tight control to the Content Provider(s) 101, a series of tools are provided to enable the Content Provider(s) 101 to prepare and securely package their Content 113 into SC(s) at their premises so that the Content 113 is secure when it leaves the Content Provider(s) 101 domain and never exposed or accessible by unauthorized parties. This allows Content 113 to be freely distributed throughout a non-secure network, such as the Internet, without fear of exposure to hackers or unauthorized parties.

[0169] The end goal of the tools for the Content Provider(s) 101 is to prepare and package a Content 113 such as a song or series of songs into Content SC(s) 850 and to package information describing the song (approved user of the song (content usage conditions 517), and promotional information for the song) into a Metadata SC(s) 820. To accomplish this, the following set of tools are provided:

[0170] Work Flow Manager 154 - Schedules processing activities and manages the required synchronization of processes, Preprocessing (for an audio example any required equalization, dynamic adjustment, or re-sampling) encoding and compression.

[0171] Metadata Assemblation and Entry Tool 161 - A collection of tools used to gather Content 113 description information from the Database 150 of the Content Provider(s) and/or third party databases or data import files and/or via operator interaction and provides means for specifying content usage conditions 517. Also provided is an interface for capturing or extracting content such as digital audio content for CDs or DLP files. A Quality Control Tool enables to preview of prepared content and metadata. Any corrections needed to the metadata or re-alignment of the content for further processing can be conducted.

[0172] SC(s) Packer Tool 162 - Encrypts and packages all Content 113 and information and calls the SC(s) Packer to pack into SC(s).

[0173] Content Dispensation Tool (not shown) - Dispenses SC(s) to designated distribution centers, such as Content Hosting Site(s) 111 and Electronic Digital Content Store(s) 103.

[0174] Content Promotion Web Site 153 stores Metadata SC(s) 820 and, optionally, additional promotional material for download by authorized Electronic Digital Content Store(s) 103.

B. Work Flow Manager 154

[0175] The purpose of this tool is to schedule, track, and manage Content 113 processing activities. This application enables multi-user access as well as allowing scheduling of Content 113 and status checking from remote locations within the Internet or extranet of the Content Provider(s) 101. This design also allows for collaborative processing where multiple individuals can be working on multiple pieces of Content 113 in parallel and different individuals can be assigned specific responsibilities and these individuals can be spread throughout the world.

[0176] Turning now to FIG. 8 is a block diagram of the major processes of the Work Flow Manager 154 corresponding described in this section. The work Flow Manager 154 is responsible for feeding jobs to these processes and directing jobs to the next required processes upon completion of its current process. This is accomplished through a series of Application Programming Interfaces (APIs) which such processing tool calls to:

- Retrieve the next job to process
- Indicate successful completion of a process
- Indicate unsuccessful compilation of a process and reason for the failure
- Provide status of a process (to allow initiation of processes that require only partial compilation of a dependent process)
- Add comments to a product which are made available to the designated processes

[0177] The Work Flow Manager 154 also has a user interface, an example Work Flow Manager User Interface 700 is illustrated in FIG. 7 which provides the following functions:

- a configuration panel to allow specification of default values and conditions to be assigned and performed during various stages of processing
- customization of the work flow rules and automated processing flows
- job scheduling
- status queries and reports
- add comments or instructions for a job associated to one or more processes
- job management (i.e. suspend, release, remove, change priority (code of processing))

[0173] Each process has a queue associated with it managed by the Work Flow Manager 154. All processes requesting jobs from the Work Flow Manager 154 results in the Work Flow Manager 154 either suspending the process (not) in a wait state if there are no jobs currently in its associated queue or returning to the process all information about the job needed to perform its respective process. If a process is suspended in a wait state, it resumes processing when a job is placed on its queue by the Work Flow Manager 154.

[0174] The Work Flow Manager 154 also manages the flow or order of processing based on a set of defined rules. These rules can be customized by the Content Provider(s) 101 if it has special processing requirements or configures specific default rules. When a process requests completion of its assigned task, it notifies the Work Flow Manager 154 of this status and the Work Flow Manager 154 decides what queue the job gets placed on next based on the defined rules.

[0175] Comments indicating special handling instructions or notices may also be attached to the product at any of the processing steps via either the programming API or manually through the Work Flow Manager User Interface 700 or processor interfaces.

[0176] The processes in the Work Flow Manager 154 are implemented in Java in the preferred embodiment but other programming languages such as C/C++, Assembler and equivalent can be used. It should be understood that the processes described below for the Work Flow Manager 154 can run on a variety of hardware and software platforms.

The Work Flow Manager 154 as a compiler system or as any of its constituent processes, may be distributed as an application program in a computer readable medium including but not limited to electronic distribution such as the web or on floppy diskettes, CD ROMs and removable hard disk drives.

[0177] FIG. 7 is a block diagram of the major processes of the Work Flow Manager 154 corresponding to FIG. 7. The following sections summarize each process and describes the information or action required by each process.

1. Products Awaiting Action/Information Process 801

[0178] Jobs are placed on specific processes queues once all information required by that process is available and the job has already successfully completed all dependent processing. A special queue exists in the Work Flow Manager 154 which is used to hold jobs that are not currently available for processing due to missing information or a failure that prevent further processing. These jobs are placed in the Products Awaiting Action/Information Process 801 queue. Each job in this queue has an associated status to indicate the action or information it is waiting on, the last process that worked on this job, and the next process(es) that is queued to or on the missing or additional information is provided or the required action is successfully completed.

[0179] Completion of any process causes the Work Flow Manager 154 to check the queue and determine if any job in this queue was awaiting the completion of this process (action) or information provided by this process. If so, that job is queued to the appropriate process queue.

2. New Content Request Process 802

[0180] The Content Provider(s) 101 determines those products (for example, a product may be a song or a collection of songs) it wishes to sell and deliver electronically. The initial function of the Work Flow Manager 154 is to enable an operator to identify these products and to place them on the queue of the New Content Request Process 802. The Content Provider(s) 101 may specify through configuration options, what information is prompted for on the product selection interface. Enough information is needed to uniquely identify the product. Optionally, additional fields may be selected to request manual entry of the information required to initiate the audio processing phase in parallel with the metadata acquisition, if not provided manually, this information can optionally be retrieved from default configuration settings or from the Database 160 of the Content Provider(s), obtained in the first stage of Metadata Processing as in Automatic Metadata Acquisition Process 803. The makeup and capabilities of the Content 113 in the Database 160 of the Content Provider(s) determines the Content selection process.

[0181] If the required information needed to perform a query to the Database 160 of the Content Provider(s) 101 is specified, the job is processed by the Automatic Metadata Acquisition Process 803. In a music embodiment, to properly

schedule the product for audio processing, the product's genre and the desired compression levels are specified as well as the audio PCM or WAV filename(s). This information may be entered as part of the product selection process or selected via a customized query interface or Web browser function. Specification of this information enables the product to be scheduled for content processing.

[0182] The product selection user interface provides an option enabling the operator to specify whether the product can be released for processing or whether it is held pending further information entry. If held, the job is added to the queue of the New Content Request Process 802 awaiting further action to complete data entry and/or release the product for processing. Once the product is released, the Work Flow Manager 154 evaluates the information specified and determines which processes the job is ready to be passed to.

[0183] If adequate information is provided to enable an automated query to the Database 160 of the Content Provider(s) 101, the job is queued for Manual Metadata Entry Process 803. If the database mapping table has not been configured for the Automatic Metadata Acquisition Process 803, the job is queued for Manual Metadata Entry Process 804 (see Automatic Metadata Acquisition Process 803 section for details on the Database Mapping Table).

[0184] If the required general information for audio processing and the specific information required for watermarking is specified, the job is queued for Watermarking Process 808 (the first phase of content processing). If any of the required information is missing when the job is released, the job is queued to the queue of the Products Awaiting Action/Information Process 801 along with status indicating the information that is missing.

[0185] If the status indicates that the filename of the Content 113, for example where the Content 113 is audio and the PCM or WAV file is missing, this may indicate that a capture (or digital extraction from digital media) is required. The audio processing functions require that the song file is accessible via a standard file system interface. If the songs are located on external media or a file system that is not directly accessible to the audio processing tools, the files are first to be copied to an accessible file system. If the songs are in digital format but on CD or Digital Tape, they are extracted to a file system accessible to the audio processing tools. Once the files are accessible, the Work Flow Manager User Interface 700 is used to specify or select the path and filename for the job so that it can be released to the watermarking process, assuming all other information required for watermarking has also been specified.

3. Automatic Metadata Acquisition Process 803

[0186] The Automatic Metadata Acquisition Process 803 performs a series of queries to the Database 160 of the Content Provider(s) 101 or a staging database where data has been imported. In an attempt to obtain as much of the product information as possible in an automated fashion, The Automatic Metadata Acquisition Process 803 requires the following information prior to allowing items to be placed on its queue:

- database mapping table with adequate information to generate queries to the Database 160 of the Content Provider(s) 101
- product information required to uniquely define products
- adequate product information to uniquely define queries

[0187] An automated query is performed to the Database 160 of the Content Provider(s) 101 to obtain the information necessary to process this Content 113. For example, if the Content 113 is music, the information needed to perform this query could be the album name or maybe a UPC or a specific album or selection ID as defined by the Content Provider(s) 101. Of the information to be obtained, some is designated as required (see the section on Automatic Metadata Acquisition Process 803 for details). If the required information is obtained, the job is next queued for Usage Conditions Process 805 if any required information is missing, the song is queued for Manual Metadata Entry Process 804. If any jobs in the Products Awaiting Action/Information Process 801 queue are waiting for any of the information obtained in this step, the job's status is updated to indicate that it is no longer waiting for this information. If that job no longer has any outstanding requirements, it is queued to the next defined queue.

4. Manual Metadata Entry Process 804

[0188] The Manual Metadata Entry Process 804 provides a means for an operator to enter missing information. It has no dependencies. Once all required information is specified, the job is queued for Usage Conditions Process 805.

5. Usage Conditions Process 805

[0189] The Usage Conditions Process 805 allows specification of product uses and restrictions. The Usage Conditions Process 805 may require some metadata. Upon completion of Usage Conditions specifications, the job is eligible to be queued for Metadata SC(s) Creation Process 807 unless the Supervised Release Process 806 option has been

requested or is configured as the default in the Work Flow Manager 154 rules. In that case, the job is queued for Supervised Release Process 803. Before queuing to Metadata SC(s) Creation Process 807, the Work Flow Manager 154 will ensure that all dependencies for that process have been met (see below). If not, the job is queued to the Products Waiting Action/Information Process 801.

6. Supervised Release Process 803

[0190] The Supervised Release Process 803 allows a quality check and validation of information specified for the digital content product. It does not have any dependencies. Comments previously attached to the job at any stage of the processing for this product can be reviewed by the Supervisor and appropriate action taken. After reviewing all information and comments, the Supervisor has the following option:

- approve release and queue the product for Metadata SC(s) Creation Process 807
- modify and/or add information and queue the product for Metadata SC(s) Creation Process 807
- add comments to the job and re-queue for Manual Metadata Entry Process 804
- add comments and queue the job to the queue for Products Waiting Action/Information Process 801

7. Metadata SC(s) Creation Process 807

[0191] The Metadata SC(s) Creation Process 807 gathers together all the information collected above as well as other information required for the Metadata SC(s) 620 and calls the SC(s) Packer Process to create the Metadata SC (620). This tool requires the following as input:

- the required metadata
- the usage conditions
- the encryption keys used in the encryption stage of all quality levels for this product

[0192] This last dependency requires that the associated audio objects completed the audio processing phase before the Metadata SC(s) 620 can be created. Upon completion of the Metadata SC(s) Creation Process 807, the job is queued to either the queue for Final Quality Assurance Process 813 or Content Dissemination Process 814 based on defined work flow rules.

8. Watermarking Process 808

[0193] The Watermarking Process 808 adds copyright and other information to the Content 113. For an embodiment where the Content 113 is a song, this tool requires the following as input:

- song filename(s) (multiple filenames if album)
- watermarking instructions
- watermarking parameters (information to be included in the watermark)

[0194] Upon completion of the Watermarking Process 808, the job is queued for Preprocessing and Compression Process 809 if its required input is available or otherwise queued to the Products Waiting Action/Information Process 801.

9. Preprocessing and Compression Process 809

[0195] The Preprocessing and Compression Process 809 encodes the Content 113 to the specified compression level performing any required preprocessing first. Queuing a job to this queue actually creates multiple queue entries. A job is created for each compression level of the product defined. The encoding processes can be performed in parallel on multiple systems. This tool requires the following input:

- watermarking content filename(s) (multiple filenames if Content 113 is an album)
- quality levels for product (could be pre-configured)
- compression algorithm (could be pre-configured)
- product genre (if required by preprocessor)

[0196] Upon completion of the encoding process, the jobs are queued to the Content Quality Control Process 810

If configured by the work flow rules, if not, the jobs are queued for Encryption Process 811.

[0197] If third party providers of encoding tools do not provide a method to display the percentage of the Content 113, such as audio, that has been processed or a method to indicate the amount of Content 113 that has been encoded as a percentage of the entire selection of Content 113 selected in FIG. 11 there is shown a flow diagram 1100 of a method to determine the encoding rate of Digital Content for the Content Preprocessing and Compression tool of FIG. 8. The method begins with the selection of the desired encoding algorithm and a bit rate, step 1101. Next, a query is made to determine if this algorithm and encoding rate has a previously calculated rate factor, step 1102. The rate factor is the factor used to determine the rate of compression for a specific encoding algorithm and a specific bit rate. If no previously calculated rate factor is stored, a sample of the Content 113 is encoded for a predetermined amount of time. The predetermined period of time is used to calculate a new rate factor, R_{New} . This rate of encoding for a predetermined amount of time is used to calculate a new rate factor, R_{New} . Calculating a new rate factor, R_{New} , knowing the amount of time and the amount of Content 113 encoded is $R_{New} = (\text{Length of Digital Content encoded}) / (\text{Amount of time})$, step 1103. The Content 113 is encoded and the encoding status is displayed using the previously calculated rate factor, step 1104. The Content 113 is encoded into the progression displayed using the previously calculated rate factor, $R_{Previous}$, step 1105. This current rate factor, R_{New} , is used to update the stored rate factor, $R_{New} = \text{AVERAGE OF } (R_{Previous} + R_{Current})$, step 1106. The iterative update of the rate factor enables the determination of the encoding rate to become more and more accurate with each subsequent use for a particular encoding algorithm and bit rate. The new rate R_{New} is then stored for future use, step 1107. The updating of $R_{Previous}$ may not be made if the current rate factor, $R_{Current}$, is out of range for the previously stored rate factor, $R_{Previous}$, by a given range or threshold.

[0198] The display of the encoding status can then be presented. The encoding status includes along with the current encoding rate, the display of the percentage of the total Content 113 displayed as a progression bar based on the encoding rate and the total length of the file for the Content 113. The encoding status can also include the time remaining for the encoding. The time remaining for the encoding can be calculated by dividing the encoding rate calculated $R_{Current}$ by the total length of the file for Content 113. The encoding status can be transformed to another program that may invoke the calling process. This can help supplementary programs to encode or co-operate programs on encoding be operated and be batched for processing more efficiently. It should be understood, in an alternative embodiment, that encoding can include the step of watermarking.

10. Content Quality Control Process 810

[0199] The Content Quality Control Process 810 is similar in function to the Supervised Release Process 803. It is an optional step allowing someone to validate the quality of the content processing performed thus far. This has no dependencies other than completion of the Watermarking Process 808 and the encoding portion of the Preprocessing and Compression Process 809. Upon completion of the Content Quality Control Process 810 the following options are available:

- the job can be released and queued for Encryption Process 811.
- comments can be attached and queued for Encryption Process 811.

[0200] The last option requires that the unencoded watermark version of the song file remain available until after Content Quality Control Process 810.

11. Encryption Process 811

[0201] The Encryption Process 811 calls the appropriate Secure Digital Content Electronic Distribution Rights Management function to encrypt each of the watermark/decoded song files. This process has no dependencies other than completion of all other audio processing. Upon completion of the Encryption Process 811 process, the job is queued for Content SC(s) Creation Process 812.

12. Content SC(s) Creation Process 812

[0202] The Content SC(s) Creation Process 812 Process may require some metadata files to be included in the Content SC(s) 830. If files other than the Content 113 are required, the files are gathered and the SC(s) Packer Process is called to create a Content SC(s) 830 for each compression level of the Content 113 (e.g. a song created. Upon

completion of the Content SC(q) Creation Process 812, the song is queued to either the Final Quality Assurance Process 813 or Content Disbursement Process 814 queue based on defined work flow rules.

13. Final Quality Assurance Process 813

[0203] Final Quality Assurance Process 813 is an optional step that allows a cross reference check between the associated Metadata and Content SC(q) 830 to verify that they match up correctly and that all information and Content 113 contained therein are correct. Upon completion of Final Quality Assurance Process 813, the jobs are queued for Content Disbursement Process 814. If a problem is found, the job (in most cases) has to be re-queued to the failing 14 stage. Rework at this stage is much more costly since the product has to go through re-encoding and repacking in addition to the reprocessing required to correct the problem. It is highly recommended that the prior assurance stages be used to assure the quality of the Content 113 and accuracy and completeness of the information.

14. Content Disbursement Process 814

[0204] The Content Disbursement Process 814 Process is responsible for transferring the SC(q)s to the appropriate hosting sites. After the successful transfer of the SC(q)s, the job compilation status is logged and the job is deleted from the queue. If a problem occurs in transferring the SC(q)s, after a defined number of retries, the job is flagged in the Workflow Manager Tool 154 as having failed along with the error encountered.

15. Work Flow Rules

[0205] The Work Flow Rules for FIG. 6 operate in three major systems as follows:

A: Work Flow Manager Tool 154

1. New Content Request Process 802
2. Product Awaiting Action/Information Process 801
3. Final Quality Assurance Process 813
4. Content Disbursement (and Notification) Process 814

B: Metadata Assimilation and Entry Tool 181

1. Automatic Metadata Acquisition Process 803
2. Manual Metadata Entry Process 804
3. Supervised Release Process 806
4. Metadata SC(q) Creation Process 807

C: Content Processing Tools 155

1. Watermarking Process 808 (requires copyright data)
2. Preprocessing and Compression Process 809
3. Content Quality Control Process 810
4. Encryption Process 811
5. Content SC(q) Creation Process 812

Work Flow

[0206] The Content 113 selection operator inputs a new product and it starts out queued onto A1 (New Content Request Process 802).

A1: When the Content 113 selection operator releases it to the Work Flow Manager Tool 154, then it gets queued onto B1 (the Automatic Metadata Acquisition Process 803).

A2: coming from step B1 (the Automatic Metadata Acquisition Process 803),
or step B2 (Manual Metadata Entry Process 804),
or step B3 (Supervised Release Process 806)

on its way to step B4 (the Metadata SC(q) Creation Process 807)
[needs the encryption key].

coming from step Before (the Metadata SC(q) Creation Process 807)
on its way to either step A3 (the Final Quality Assurance Process 813) or step AA (the Content Disbursement Process 814)

[needs the Content SC(q) 830].

coming from step C1 (the Watermarking Process 808)

[needs the metadata for Preprocessing and Compression Process 809].

coming from step C4 (the Encryption Process 811)

on its way to step C5 (the Content SC(q) Creation Process 812)

[needs the metadata for Content SC(q) 830 Packing].

coming from step C8 (the Content SC(q) Creation Process 812)

on its way to either step A3 (the Final Quality Assurance Process 813) or step AA (the Content Disbursement Process 814)

[needs the Metadata SC(q) 820].

A3: After step A3 (the Final Quality Assurance Process 813),
place onto queue B4 (Manual Metadata Entry Process 804),
or place onto queue B3 (Supervised Release Process 806),
or place into queue as required by the quality assurance operator.

AA: After step AA (Content Disbursement Process 814),
the Work Flow Manager Tool 154 is done for this product.

B1: After step B1 (the Automatic Metadata Acquisition Process 803),
If the metadata needed for step C1 (the Watermarking Process 808) is present, then place an entry representing

sending this product onto queue C1.

(to the following logic also)
If either 1- any required metadata is missing, or 2- there are comments directed to the manual metadata providers, then also place the product onto queue B2 (Manual Metadata Entry Process 804),

else if supervised release was requested for this product, then place the product onto queue B3 (Supervised Release Process 806).

else if the product has all the information for all of the requested quality levels, then place the product onto queue Before (the Content Processing Tools 155 for Content Processing Tools 809),
else tag the product as needs the encryption key and place the product onto queue A2 (Products Awaiting Action/Information Process 801).

B2: During step B2 (Manual Metadata Entry Process 804),
If step C1 (the Watermarking Process 808) has not been done and the metadata needed for step C1 is

present, then place an entry representing this product onto queue C1.
(to the following logic also)

If metadata needed for step C2 (the Preprocessing and Compression Process 809) just been provided, then
(to the following logic also)

If all the metadata that can be gathered by the Metadata Assimilation and Entry Tool 181 is present, then
If supervised release was requested for this product, then place the product onto queue B3 (Supervised Release Process 806)

else
If all the information from step C4 (the Encryption Process 811) of the Content Processing Tools 155 is present, then place this product onto queue Before (the Metadata SC(q) Creation Process 807)
else tag the product as needs the encryption key and place the product onto queue A2 (Products Awaiting Action/Information Process 801).

else
If the metadata provider requested a forced supervised release, then place the product onto queue

B3 (Supervised Release Process 806)
else do nothing (keep the product on queue B2 (Manual Metadata Entry Process 804)).

B3: During step B3 (Supervised Release Process 806),
If this operator is sending the product back to step B2 (Manual Metadata Entry Process 804), then place the product onto queue B2.

else if this operator released the product, then
If all the information from step C4 (the Encryption Process 811) of the Content Processing Tools 155
is present, then place this product onto queue Before (the Metadata SC(q) Creation Process 807)
else tag the product as needs the encryption key and place this product onto queue A2 (Products

Awaiting Action/Information Process 801).

else the product remains on queue B3 (Supervised Release Process 806).

Before/After step Before (the Metadata SC(e) Creation Process 807), flag the product. Metadata has been packed.

If all the (product/quality level) tuples have been packed, then

If the Content Provider(s) 101 configuration specifies Quality Assurance the SC(e), then place this product

onto queue A3 (the Final Quality Assurance Process 813).

else flag the product as needs the Content Dissemination Process 814).

Action/Information Process 801).

C1: After step C1 (the Watermarking Process 808),

If the metadata is needed for step C2 (the Preprocessing and Compensation Process 809) is present, then create an entry for each (product/quality level) tuple and place them onto queue C2.

else flag the product as needs the Preprocessing/Compensation and place this product onto queue A2 (Products Awaiting Action/Information Process 801).

C2: After step C2 (the Preprocessing and Compensation Process 809),

If the Content Provider(s) 101 configuration specifies Content Quality Control Process 810, then place this (product/quality level) tuple onto queue C3 (the Content Quality Control Process 810).

else place this (product/quality level) tuple onto queue C4 (the Encryption Process 811).

C3: After step C3 (the Content Quality Control Process 810), then place this (product/quality level)

else flag the product as needs the metadata for Content SC(e) 820 Packing and place this (product/quality level) tuple onto C2 (the Encryption Process 811).

C4: After step C4 (the Encryption Process 811),

provide the needed information (i.e., the Symmetric Key 823 generated by the Process and used to encrypt the Content 113) to the Metadata Assembler and Entry Tool 811.

If all the metadata that's required for the Content SC(e) 820 is present, then place this (product/quality level) tuple onto queue C5 (the Content SC(e) Creation Process 812).

else flag the product as needs the metadata for Content SC(e) 820 Packing and place this (product/quality level) tuple onto C2 (the Content SC(e) Creation Process 812).

C5: After step C5 (the Content SC(e) Creation Process 812),

flag the quality level of the Content 113 at this quality level has been packed.

If all the (product/quality level) tuples have been packed, then

If the product is flagged Metadata has been packed, then

product onto queue A3 (the Final Quality Assurance Process 813).

else place this product onto queue A4 (the Content Dissemination Process 814).

Awaiting Action/Information Process 801).

else flag the product as needs the Metadata SC(e) 820 and place this product onto queue A2 (Products

tuple triggers an action).

40 C. Metadata Assemblment and Entry Tool

[0207] Metadata consists of the data describing the Content 113 for example in music, title of the recording, artist, author/performer, producer and length of recording. The following description is based upon Content 113 being music but it should be understood by those skilled in the art that other content types (e.g., video, programs, multimedia, movies, and equivalent), are within the true scope and meaning of the present invention.

[0208] This Subsystem brings together the data the Content Provider(s) 101 provides to the Electronic Digital Content Store(s) 103 to help promote the sale of the product (e.g., for music, sample clip by this artist, history of this artist, provider(s), 101 provides to the End-User(s) with the purchased product (e.g., artist, producer, album cover, track length), and the different purchase options (the Usage Conditions 517) the Content Provider(s) 101 wants to offer the End-User(s). This data is packaged into a Metadata SC(e) 820 and made available to the Electronic Digital Content Store(s) 103. To accomplish this, the following tools are provided:

- Automatic Metadata Acquisition Tool
- Manual Metadata Entry Tool
- Usage Conditions Tool
- Supervised Release Tool

[0209] These tools enable Content Provider(s) 101 to implement the processes described above for Work Flow Manager 154. Tools described here are a toolkit based on Java in the preferred embodiment but other programming languages such as C/C++ , Assembler and equivalent can be used.

1. Automatic Metadata Acquisition Tool

[0210] The Automatic Metadata Acquisition Tool provides a user the ability to implement the Automatic Metadata Acquisition Process 803 described above. The Automatic Metadata Acquisition Tool is used to access the Database 180 or the Content Provider(s) 101 and to retrieve as much data as possible without operator assistance. Configuration methods are available to automate this process. The Content Provider(s) 101 can tailor the default metadata template to identify the types of data that Content Provider(s) 101 wants to provide to End-User(s) (e.g., composer, producer, statement, track length) and the types of promotional data the Content Provider(s) 101 provides to the Electronic Digital Content Store(s) 103 (e.g., for a music example, sample clips by this artist, a list of albums on which this recording appears, genres associated with the artist). The default metadata template include data fields which are required by the End-User Device(s) 110, data fields which can be optionally provided to the End-User Device (e.g.) 109 and a sample set of data fields, targeted to the Electronic Digital Content Store(s) 103, that promote the artist, album, artist, single.

[0211] To extract the template data fields from the Database 180 of the Content Provider(s) 101 the Automatic Metadata Acquisition Tool uses a table that maps the type of data found (e.g., composer, producer, a biography of the artist) to the location within the database where the data can be found. Each of the Content Provider(s) 101 help specify that mapping table for their environment.

[0212] The Automatic Metadata Acquisition Tool uses a metadata template of the Content Provider(s) 101 and mapping table to acquire whatever data is available from the Database 180 of the Content Provider(s) 101. The status of each product is updated with the result of the Automatic Metadata Acquisition Process 803. A product which is in making requested, then the product is available for packing into a Metadata SC(e) 820.

2. Manual Metadata Entry Tool

[0213] The Manual Metadata Entry Tool provides a user the ability to implement the Manual Metadata Entry Process 804 described above. The Manual Metadata Entry Tool allows any properly authorized operator to provide the marketing and request supervised release. The Content Provider(s) 101 may require, for quality assurance reasons, that the product undergo supervised release. Once all the required data is present, and if supervised release has not been requested, then the product is available for packing into a Metadata SC(e) 820.

3. Usage Conditions Tool

[0214] The Usage Conditions Tool provides a user the ability to implement the Usage Conditions Process 805 described above. The process of offering Content 113 for sale or rent (limited use), using electronic delivery, involves a series of business decisions. The Content Provider(s) 101 decides at which compression level(s) the Content 113 is made available. Then for each compressed encoded version of the Content 113 one or more usage conditions are specified. Each usage condition defines the rights of the End-User(s), and any restrictions on the End-User(s), with regard to the use of the Content 113.

[0215] As part of Content Processing Tools 155, a set of usage conditions (End-User(s) rights and restrictions) is attached to the product.

[0216] A usage condition defines:

1. the compression encoded version of the Content 113 to which this usage condition applies.
2. the type of user covered by this usage condition (e.g., business, private consumer)
3. whether this usage condition allows for the purchase or the rental of the Content 113.

For a rental transaction:

- the measurement unit which is used to limit the term of the rental (e.g., days, plays).
- the number of the above units after which the Content 113 will no longer play.

the number of playable copies the End-User(s) is allowed to make, onto what kinds of media can (s)he make those copies (e.g., CD-Recordable (CD-R), MiniDisc, Personal Computer).

4. the period of time during which the purchase/rental transaction is allowed to occur (i.e., an End-User(s) can purchase/rent under the terms of this usage condition only after the beginning availability date and before the last date of availability);

5. the countries from which an End-User(s) can transact this purchase (or rental);

6. the price of the purchase/rental transaction under this usage condition 7. the watermarking parameters;

8. the types of events which require notification of the Clearinghouse(s) 105.

An Example of a Set of Usage Conditions

[0217] The Content Provider(s) 101 may decide to test the North American market's acceptance to the re-release of the children's song by a popular children's vocalist during the fourth quarter 1997. The test will make the song available in two different compression encoding versions: 384Kbps and 56Kbps. The 384Kbps version can be bought (and one copy made onto MiniDisc) or rented (for two weeks), while the 56Kbps version can only be bought (and no copies made). The watermarking instructions is the same for any purchase/rental, and the Content Provider(s) 101 wants the Clearinghouse(s) 105 to count every copy made. This would create Usage Conditions as follows:

	Usage Condition 1	Usage Condition 2	Usage Condition 3
compression encoded	384Kbps	384Kbps	56Kbps
version			
type of user	private consumer	private consumer	private consumer
type of transaction	purchase	rental	purchase
availability dates	1 Oct 1997 - 31 Dec 1997	1 Oct 1997 - 31 Dec 1997	1 Oct 1997 - 31 Dec 1997
countries	USA and Canada	USA and Canada	USA and Canada
watermarking	std.	std.	std.
notifying events	copy action	none	none
number of copies	1	0	0
onto what media	MiniDisc	not applicable	not applicable
term of rental	not applicable	14 days	not applicable
price	Price 1	Price 2	Price 3

4. Parts of the Metadata SC(s) 820

[0218] Below are some of the kinds of data that the Metadata Administration and Entry Tool 101 gathers for inclusion into the Metadata SC(s) 820. An attempt has been made to group the data into SC(s) parts by function and destination.

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

205

206

207

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

224

225

226

227

228

229

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

256

257

258

259

260

261

262

263

264

265

266

267

268

269

270

271

272

273

274

275

276

277

278

279

280

281

282

283

284

285

286

287

288

289

290

291

292

293

294

295

296

297

298

299

300

301

302

303

304

305

306

307

308

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328

329

330

331

332

333

334

335

336

337

338

339

340

341

342

343

344

345

346

347

348

349

350

351

352

353

354

355

356

357

358

359

360

361

362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

392

393

394

395

396

397

398

399

400

401

402

403

404

405

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

425

426

427

428

429

430

431

432

433

434

435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

462

463

464

465

466

467

468

469

470

471

472

473

474

475

476

477

478

479

480

481

482

483

484

485

486

487

488

489

490

491

492

493

494

495

496

497

498

499

500

501

502

503

504

505

506

507

508

509

510

511

512

513

514

515

516

517

518

519

520

521

522

523

524

525

526

527

528

529

530

531

532

533

534

535

536

537

538

539

540

541

542

543

544

545

546

547

548

549

550

551

552

553

554

555

556

557

558

559

560

561

562

563

564

565

566

567

568

569

570

571

572

573

574

575

576

577

578

579

580

581

582

583

584

585

586

587

588

589

590

591

592

593

594

595

596

597

598

599

600

601

602

603

604

605

606

607

608

609

610

611

612

613

614

615

616

617

618

619

620

621

622

623

624

625

626

627

628

629

630

631

632

633

634

635

636

637

638

639

640

641

642

643

644

645

646

647

648

649

650

651

652

653

654

655

656

657

658

659

660

661

662

663

664

665

666

667

668

669

670

671

672

673

674

675

676

677

678

679

680

681

682

683

684

685

686

687

688

689

690

691

692

693

694

695

696

697

698

699

700

701

702

703

704

705

706

707

708

709

710

711

712

713

714

715

716

717

718

719

720

721

722

723

724

725

726

727

728

729

730

731

732

733

734

735

736

737

738

739

740

741

742

743

744

745

746

747

748

749

750

751

752

753

754

755

756

757

758

759

760

761

762

763

764

765

766

767

768

769

770

771

772

773

774

775

776

777

778

779

780

781

782

783

784

785

786

787

788

789

790

791

792

793

794

795

796

797

798

799

800

801

802

803

804

805

806

807

808

809

810

811

812

813

814

815

816

817

818

819

820

821

822

823

824

825

826

827

828

829

830

831

832

833

834

835

836

837

838

839

840

841

842

843

844

845

846

847

848

849

850

851

852

853

854

855

856

857

858

859

860

861

862

863

864

865

866

867

868

869

870

871

872

873

874

875

876

877

878

879

880

881

882

883

884

885

886

887

888

889

890

891

892

893

894

895

896

897

898

899

900

901

902

903

904

905

906

907

908

909

910

911

912

913

914

915

916

917

918

919

920

921

922

923

924

925

926

927

928

929

930

931

932

933

934

935

936

937

938

939

940

941

942

943

944

945

946

947

948

949

950

951

952

953

954

955

956

957

958

959

960

961

962

963

964

965

966

967

968

969

970

971

972

973

974

975

976

977

978

979

980

981

982

983

984

985

986

987

988

989

990

991

992

993

994

995

996

997

998

999

1000

the period of time during which the purchase/rental transaction is allowed to occur (i.e., an End-User(s) can purchase/rent under the terms of this usage condition **only** after the beginning availability date and before the last date of availability)

5 a pointer to the countries from which an End-User(s) can transact this purchase (or rental)

10 the price of the purchase/rental transaction under this usage condition

15 a pointer to the types of events which require notification of parameters

20 purchase data (encrypted; optional info; src: EMS; dest: end-user, Clearinghouse(s) 105)

25 purchase price

bill to name and address

consumer name and address

country of the consumer (best guess)

30 metadata 1 (src: content provider; dest: EMS, end-user)

35 an array of {

40 copyright information for the composition for the sound recording title of song principal artist(s) }

45 a pointer to { the artwork (e.g., album cover); the format of the artwork (e.g., GIF, JPEG); }

50 optional info:

55 an array of additional information {

60 composer publisher producer }

65 sidemen

date of recording

date of release

lyrics

70 track name (description) / track length

list of albums on which this recording appears

75 genre(s) }

80 metadata 2 (src: content provider; dest: EMS)

85 an array of structures, each representing different quality levels of the same sound recording {

90 the quality level of the sound recording; the size (in bytes) of the (probably compressed) sound recording,

95 }

100 metadata 3 (src: content provider; dest: EMS, end-user)

105 optional info:

110 promotional material:

115 a pointer to artist promotion material {

120 a URL to the artist's web site;

125 background description(s) of the artist(s); artist-related interviews (along with format of the interview (e.g., text, audio, video));

130 reviews (along with format of the reviews (e.g., text, audio, video)); sample clips (and its format and compression level); recent and upcoming concerts/appearances/events - their dates and locations;

135 }

140 a pointer to album promotion material {

145 sample clip (and its format and compression level); background description(s) of the producer, and/or the composer, and/or the movie/play/cast, and/or the making of the album, etc.;

150 non-artist-related interviews (along with format of the interview (e.g., text, audio, video));

reviews (along with format of the reviews (e.g., text, audio, video)), sample clip (and its format and compression level) background description(s) of the producer, and/or the composer, and/or the movie/play/cast, and/or the making of the single, etc.

15 reviews (along with format of the reviews (e.g., text, audio, video))
 20 5. Supervised Release Tool
 25 [0219] Supervised Release Tool provides a user the ability to implement the Supervised Release Process 808 described above. An individual designated by the Content Provider(s) 101 as having supervised release authority, may call up a product awaiting supervised release (i.e., a product on the queue of the Supervised Release Process 808), examine its Content 113 and its accompanying comments, and either approve its Content 113 and release the product for packing into a Metadata SC(0) 620, or make any necessary corrections and release the product for packing into a Metadata SC(0) 620 or add a comment specifying the corrective action to take and resubmit the product to the Manual Metadata Entry Process 704.

30 [0220] In another embodiment, after the creation of the SC(0)s, there is another optional quality assurance step where the Content 113 of the SC(0)s can be opened and examined for completeness and accuracy, and, at that time, final approval can be given or denied for the product's release to the retail channel.

D. Content Processing Tools

35 [0221] The Content Processing Tools 155 is actually a collection of software tools which are used to process the digital content file to create watermarking, encoded, and encrypted copies of the content. The tools makes use of industry standard digital content processing tools to allow plugable replacement of watermarking, encoding, and encryption technologies as they evolve. If the selected industry tool can be loaded via a command line, system call interface and passed parameters or provides a toolkit wherein functions can be called via a DLL interface, the content processing can be automated to some degree. A front end application to each tool queries the appropriate queue in the Content Processing Tools 155 for the next available job, retrieves the required files and parameters and then loads the industry standard content processing tool to perform the required function. Upon completion of the task, manual update to the queue may be required if the tool does not report terminating status.

40 [0222] A generic version of the Content Processing Tools 155 is described, but customization is possible. The Content Processing Tools 155 can be written in Java, C/C++ or any equivalent software. The Content Processing Tools 155 can be delivered by any computer readable means including diskettes, CDS or via a Web site.

1. Watermarking Tool

45 [0223] The Watermarking Tool provides a user the ability to implement the Watermarking Process 808 as described above. This tool applies copyright information of the Content 113 owner to the song file using audio Watermarking technology. The actual information to be written out is determined by the Content Provider(s) 101 and the specific watermarking technology selected. This information is available to the front end Watermarking Tool so that it can properly pass this information to the watermarking function. This imposes a synchronization requirement on the Metadata Administration and Entry Tool 161 to assure that it has acquired this information prior to, for example, allowing the song's audio file to be processed. This song will not be available for audio processing until the watermarking information has

been obtained.

[0224] The watermark is applied as the first step in audio processing since it is common to all encodings of the song created. As long as the watermark can survive the encoding technology, the watermarking process need only occur once per song.

[0225] Various watermarking technologies are known and commercially available. The front end Watermarking Tool through is capable of supporting a variety of industry Watermarking tools.

2. Preprocessing and Compression Tool

50 10 [0226] The Preprocessing and Compression Tool provides a user the ability to implement the Preprocessing and Compression Process 809 as described above. Audio encoding involves two processes. Encoding is basically the application of a lossy compression algorithm (e.g., for a music download example, a PCM audio stream). The encoder can usually be tuned to generate various playback bit stream rates based on the level of audio quality required. Higher quality results in larger file sizes and since the file sizes can become quite large for high quality Content 113, download times for high quality Content 113 can become lengthy and sometimes prohibitive on standard 28,800 bps modems.

15 [0227] The Content Provider(s) 101 may, therefore, choose to offer a variety of digital content qualities for download to appease both the impatient and low bandwidth customers who don't want to wait hours for a download and the audiophile or high bandwidth customers who either only buy high quality Content 113 or has a higher speed connection.

20 [0228] Compression algorithms vary in their techniques to generate lower bit rate reproductions of Content 113. The techniques vary both by algorithm (i.e. MP3, AC3, ATRAC) and by levels of compression. To achieve higher levels of compression, typically the data is re-sampled at lower sampling rates prior to being delivered to the compression algorithm. To allow for more efficient compression with less loss of fidelity or to prevent drastic dropout of some frequency ranges, the digital content may sometimes require adjustments to equalization levels of certain frequencies or adjustments to the dynamics of the recording. The content preprocessing requirements are directly related to the compression algorithm and the level of compression required. In some cases, the style of Content 113 (e.g. musical genre) can be successfully used as a base for determining preprocessing requirements since songs from the same genre typically have similar dynamics. With some compression tools, the preprocessing functions are part of the encoding process, with others, the desired preprocessing is performed prior to the compression.

25 [0229] Besides the downloadable audio file for sale, each song also has a Low Bit Rate (LBR) encoded clip to allow the song to be sampled via a LBR streaming protocol. This LBR encode is also the responsibility of the Content Processing Tools 155. This clip is either provided by the Content Provider(s) 101 as a separate PCM file or as a parent file of offset and length.

30 [0230] As with watermarking, it is hoped that the encoding tools can be loaded via a DLL or command line system call interface and passed all the required parameters for preprocessing and compression. The front end Encoding Tool may have a synchronization requirement with the Metadata Administration and Entry Tool 161 for example if the content is music, and if it is determined that the song's genre is acquired from the Database 160 of the Content Provider(s) prior to performing any audio preprocessing. This depends on the encoding tools selected and how indeterminate the genre for the song is. If the Content Provider(s) 101 varies the choice of encoder/quality levels per song, this information is also be provided prior to the encoding step and agrees with the metadata being generated by the Metadata Administration and Entry Tool 161.

35 [0231] A variety of high quality encoding methods and tools are known today. The front end Encoding Tool though is capable of supporting a variety of industry encoding tools.

40 [0232] Turning now to FIG. 12 is shown a flow diagram of one embodiment for the Automatic Metadata Acquisition Tool of FIG. 8 according to the present invention. The process starts with reading an identifier from the media the Content Provider(s) 101 is examining. One example of content in an audio CD embodiment, in an audio CD embodiment, the following codes may be available Universal Price Code (UPC), International Standard Recording Code (ISRC), International Standard Music Number (ISMN). This identifier is read in the appropriate player for the content, for example an audio CD player for audio CD, DVD player for DVD movie, DAT recorder for DAT recording and a turntable.

45 [0233] Turning now to FIG. 12 is shown a flow diagram of one embodiment for the Automatic Metadata Acquisition Tool of FIG. 8 according to the present invention. The process starts with reading an identifier from the media the Content Provider(s) 101 is examining. One example of content in an audio CD embodiment, in an audio CD embodiment, the following codes may be available Universal Price Code (UPC), International Standard Recording Code (ISRC), International Standard Music Number (ISMN). This identifier is read in the appropriate player for the content, for example an audio CD player for audio CD, DVD player for DVD movie, DAT recorder for DAT recording and a turntable. Step 1201. Next this identifier is used to index a Database 160 for the Content Provider(s) 101, step 1202. Some or all of the information required by the Work Flow Manager Process as described in FIG. 8 is retrieved in Database 160 and any other related sources, step 1203. This information can include the Content 113 and the metadata related to it. In step 1204, the additional information retrieved is used to start the Work Flow Manager 154 for creating electronic Content 113. It should be understood, that several selections of media, such as several audio CDS, can be queued up so as to enable the Automatic Metadata Acquisition Tool to create a series of Content 113 for electronic distribution.

50 45 For example, all the Content 113 could be created from a series of CDS or even selected tracks from one or more CDS examined by the Content Provider(s) 101.

55 [0233] In an alternate embodiment, the preprocessing parameters can be retrieved from the Database 160 of the Content Provider(s) automatically. Referring now to FIG. 13 is a flow diagram of a method to automatically set the

Preprocessing and Compression parameters of the Preprocessing and Compression Tool of FIG. 8 according to the present invention. In this embodiment, the Content 113 is music. In step 1301, music (Content 113) is selected to be encoded in Content Processing Tools 155. The genre of the music selected is determined, step 1302. This can be entered manually or by using other meta data available, such as the additional data retrieved from the process described in FIG. 12. The audio compression level and audio compression algorithms selected are then examined, step 1303. Next, a backup is made by genre, compression settings and compression algorithms of what compression parameters should be used in the Preprocessing and Compression Process 809, 1304.

3. Content Quality Control Tool

[0244] The Content Quality Control Tool provides a user the ability to implement the Content Quality Control Process 810 as described above. This is an optional Content Processing tool and provides an opportunity for a quality control technician to review the encoded and watermarked content files and approve or reject the content files based on quality judgments. He can re-select the content making minor preprocessing adjustments until the quality is adequate or can flag the song for reprocessing and attach a note describing the problem.

[0245] This process step can be configured by the Content Provider(s) 101 as an optional or required step of the content processing work flow. An additional optional Final Quality Assurance Process 813 step is provided after packaging of all the SC(s) for this content (e.g. each SC(s) for song on a CD) at which time the quality of the content encoding can be tested but catching a problem early prior to encryption and packaging allows for more efficient content processing. It is, therefore, highly desirable that the content quality be assured at this step as opposed to waiting until final completion of all processing.

4. Encryption Tool

[0246] The Encryption Tool provides a user the ability to implement the Encryption Process 811 as described above. Content encryption is the final step of the Content Processing Tools 155. Each of the variations of the content that were created by the Encoding Tool is now encrypted. The encryption tool is a function of the SC(s) Packer. The SC(s) Packer is called to encrypt the song and returns the generated encryption key used. This key is later passed into the SC(s) Packer for use in creation of the Metadata SC(s) 820.

E. Content SC(s) Creation Tool

[0247] Once all metadata has been gathered the Content SC(s) Creation Tool groups the metadata into categories based on their intended use. These groups of metadata are written into files to be passed in to the SC(s) Packer tool as Metadata parts for the Metadata SC(s) 820. Each part (file) has unique processing requirements. Once the associated songs have been processed, and encrypted and the target destination (URL of Content Hosting Site(s) 111) has been determined, the Content SC(s) 820 for the Content 113 are ready to be created. The Content 113 thus have completed processing and have met all the requirements described above, are queued for packing in the packet queue of the Work Flow Manager 154.

[0248] The Content SC(s) Creation Tool now retrieves all the required files created by the previous steps of the Metadata Administration and Entry Tool 161 and calls the SC(s) Packer functions to create the Metadata SC(s) 820 and Content SC(s) 830. This process creates a single Metadata SC(s) 820 and multiple Content SC(s) 830 for each song. For example, if the content is music, each of the audio files created during audio processing for the various quality levels of the full song is packed into separate Content SC(s) 830. The audio file created for the sample clip is passed as a metadata file to be included in the Metadata SC(s) 820.

F. Final Quality Assurance Tool

[0249] The Final Quality Assurance Tool provides a user the ability to implement the Final Quality Assurance Process 813 as described above. Once all the SC(s) have been built for a content file, the content is available for a final quality assurance check. Quality assurance can be performed at various stages of the Content 113 preparation process. The Content Provider(s) 101 can choose to perform quality assurance as each major step completed to prevent excessive rework later or may choose to wait until all audio preparation processes are complete and perform quality assurance on everything at once. If the latter is chosen, quality assurance is performed at this point in compilation of the creation of the SC(s). This tool allows each SC(s) for the song to be opened, examined, and the audio played.

[0250] Any problem discovered, even minor (text changes) requires that the SC(s) be rebuilt due to internal security features of SC(s). To avoid unnecessary reprocessing time, it is highly recommended that the first quality assurance step be utilized to assure accuracy of the metadata and that this specific quality assurance step be reserved for

validating appropriate cross references between the SC(s) associated with this song. If problems are found, the assurer can enter a problem description to be attached to the song and have it re-queried to the appropriate processing queue for reprocessing. Status is updated appropriately in the Work Flow Manager 154 to indicate the status of all related components of the song. If no problems are discovered, the Content 113 is marked or flagged as ready for release.

G. Content Dispersal Tool

[0244] The Content Dispersal Tool provides a user the ability to implement the Content Dispersal Process 814 as described above. Once the Content 113 has been approved for release, the SC(s) for the Content 113 are placed in the queue of the Content Dispersal Process. The Content Dispersal Tool monitors the queue and performs immediate transfer of the SC(s) files or batch transfer of a group of SC(s) files based on the configuration settings provided by the Content Provider(s) 101. The Content Provider(s) 101 can also optionally configure the Content Dispersal Tool to automatically hold all SC(s) in this queue until they are manually flagged for release. This allows the Content Provider(s) 101 to prepare content in advance of their scheduled release date and hold them until they wish to release them, e.g., a new song, movie or game. The Content Provider(s) 101 can also control access to Content 113 based on defined release date so there is no requirement for the Content Provider(s) 101 to actually hold up delivery of the SC(s) but this manual release option can still be used for this purpose or used to manage network bandwidth required to transfer these large files.

[0245] When trigger for release, the Content SC(s) 830 for the Content 113 are transferred via FTP to the designated Content Hosting Site(s) 111. The Metadata SC(s) 820 is transferred via FTP to the Content Promotions Web Site 158. Here the SC(s) are staged to a new Content 113 directory until they can be processed and integrated into the Content Promotions Web Site 158.

[0246] FIG. 17 is a flow diagram of an alternate embodiment to automatically retrieve additional information for the Automatic Metadata Acquisition Tool of FIG. 8 according to the present invention. The process is similar for that described in FIG. 8 above. However, the quality checks of Supervised Release 808 and Content Quality Control 809 are combined into one quality check called Quality Control 807. Performing quality check prior to SC creation, eliminates the steps of unpacking the Content 113 and the associated Metadata SC(s) 820. In addition, in this embodiment, the queue of Products Available Information 801 have been eliminated. The jobs are placed on the specific process queues depending on what action is being requested. For example, if the job requires Manual Metadata, i.e. additional Metadata to be entered, the job is placed on the Manual Metadata entry queue. Also the Automatic Metadata Acquisition 803 has been merged with New Content Request to occur up front to the Metadata Administration and Entry Tool 161 and the Content Processing Tool 155. Finally, it is important to point out that the Usage Conditions 804 are enlarged both at the Automatic Metadata Acquisition 803 and during the Manual Metadata Entry 803. Since, many of the usage conditions can be automatically filled-in during the Automatic Metadata Acquisition 803 step.

H. Content Promotions Web Site

[0244] To most effectively disperse information on what the Content Provider(s) 101 is making available for sale via digital download, and to get the necessary files to the Electronic Digital Content Store(s) 103 to enable it to make this Content 113 available for download to its customer, each Content Provider(s) 101 should have a secure web site containing this information. This is similar to the method used today by some Content Provider(s) 101 to make promotional content available to their sellers and others with a need for this information. In the case where this type of service already exists, an additional section and others with a need to the web site where Electronic Digital Content Store(s) 103 can go to see a list of the content available for sale via download.

[0245] The Content Provider(s) 101 has complete control over the design and layout of this site or can choose to use a turnkey web server solution provided as part of the toolkit for Secure Digital Content Electronic Distribution System 100. To implement their own design for this service, the Content Provider(s) 101 need only provide links to the Metadata SC(s) 820 for Electronic Digital Content Store(s) 103 who access their site. This is accomplished using the Content Provider(s) 101 to select the content to be displayed or extract information from the container. The information can then be used to update HTML Web pages and/or add information to a searchable database maintained by this service. The SC(s) Preview Tool is actually a subset of the Content Acquisition Tool used by the Electronic Digital Content Store(s) 103 to open and process Metadata SC(s) 820. See the Content Acquisition Tool section for more detail. The Metadata SC(s) 820 file should then be moved to a permanent directory maintained by the Content Promotions Web Site 158.

[0247] Once the Metadata SC(s) 620 has been integrated into the Content Promotions Web Site 156, its availability is published. The Content Provider(s) 101 can send a notification to all subscribing Electronic Digital Content Store(s) 103 as each new Metadata SC(s) 620 is added to the site or can perform a single notification daily (or any defined periodicity) of all Metadata SC(s) 620 added that day (or period). This notification is performed via a standard HTTP exchange with the Electronic Digital Content Store(s) 103 Web Server by sending a defined CGI string containing parameters referencing the Metadata SC(s) 620 added. This messaging is handled by the Notification Interface Module of the Electronic Digital Content Store(s) 103 which is described later.

1. Content Hosting

[0248] The Entertainment Industry produces thousands of content titles, such as CDs, movies and games every year, adding to the tens of thousands of content titles that are currently available. The Secure Digital Content Electronic Distribution System 100 is designed to support all of the content titles available in stores today.

[0249] The numbers of content titles that the Secure Digital Content Electronic Distribution System 100 may eventually download to customers on a daily basis is in the thousands or tens of thousands. For a large number of titles, this requires a large amount of bandwidth. The computer disk space and bandwidth need is call for a distributed, scalable implementation with multiple Content Hosting Site(s) 111. The system also supports customers all over the world. This requires over tens sites to speed delivery to the global customer.

[0250] Content hosting on the Secure Digital Content Electronic Distribution System 100 is designed to allow the Content Provider(s) 101 to either host their own Content 113 or share a common facility or a set of facilities.

[0251] Content hosting on the Secure Digital Content Electronic Distribution System 100 consists of multiple Content Hosting Site(s) 111 that collectively contain all of the Content 113 offered by the Secure Digital Content Electronic Distribution System 100 and several Secondary Content Sites (not shown) that contain the current hot bits offered by the Content Provider(s) 101. The number of Content Hosting Site(s) 111 changes depending on the number of End-User(s) using the system. The Secondary Content sites host a limited number of songs, but they will represent a large percentage of the bandwidth used on the system. The secondary sites are brought on line as the volume on the primary site increases to the point of maximum capacity. The secondary sites can be located close to Network Access Points (NAPs) which helps speed up download times. They may also be placed in different geographic areas around the world to speed up download times.

[0252] Should the Content Provider(s) 101 choose to host all of their Content 113 in their own system, they can act as a single Content Hosting Site 111 with or without additional Secondary Content Sites. This allows them to build their own scalable distributed system. In another embodiment, Electronic Digital Content Store(s) 103 can also act as Content Hosting Site(s) 111 for Content 113. This embodiment requires a special financial agreement between the Electronic Digital Content Store(s) 103 and the Content Provider(s) 101.

1. Content Hosting Sites

[0253] Content 113 is added to the Content Hosting Site(s) 111 via FTP or HTTP by the Content Distribution Tool described in the Content Provider(s) Section of this specification or via offline means such as content delivery on tape, CD ROM, flash, or other computer readable media. The Metadata SC(s) 620 created by the Content Provider(s) 101 contain a field that indicates the URL location of the Content SC(s) 630 for this Content 113. This URL corresponds to a Content Hosting Site(s) 111. Electronic Digital Content Store(s) 103 can overwrite this URL if allowed by the Content Provider(s) 101 in the Offer SC(s) 641. The End-User Device(s) 108 communicates to this Content Hosting Site(s) 111 when it wants to download the Content SC(s) 630.

[0254] The End-User Device(s) 108 initiates the request for a Content SC(s) 630 by sending the License SC(s) 660 to the Content Hosting Site(s) 111. This is the same License SC(s) 660 returned by the Clearinghouse(s) 105. The Digital Signature of the License SC(s) 660 can be verified to determine if it is a valid License SC(s) 660. If it is a valid License SC(s) 660 either the download is initiated, or the download request may be redirected to another Content Hosting Site(s) 111.

2. Content Hosting Site(s) 111 provided by the Secure Digital Content Electronic Distribution System 100

[0255] For the Secure Digital Content Electronic Distribution System 100 the decision of which site should be used to download the Content 113 is made by the primary content site that received the initial request for a Content SC(s) 630. This site uses the following information to make this decision:

- Are there secondary content sites that host the Content 113 requested? (The majority of Content 113 offered by the Secure Digital Content Electronic Distribution System 100 is only located at primary sites);

Where is the End-User Device(s) 109 geographically located? (This information can be obtained from the End-User Device(s) 109 when the request is initiated at the End-User Device(s) 109, this is passed up to the Clearinghouse(s) 105 in the Order SC(s) 650; is the appropriate secondary site up and operational? (Sometimes the secondary sites may be off-line); What is the load of the secondary sites? (In some cases where a secondary site is swamped with activity another site that is less busy may be selected).

[0256] Before transmitting the Content SC(s) 630 to the End-User Device(s) 109, analysis and verifications are performed on the End-User(s) request. A database is kept of all of the License SC IDs that have been used to download Content 113. This database can be checked to ensure that the End-User Device(s) 109 only makes one request for each piece of Content 113 purchased. This prevents malicious users from repeatedly accessing the Content Hosting Site(s) 111 in hopes of slowing down the Content Hosting Site(s) 111 and prevents unauthorized download of the Content SC(s) 630.

[0257] The promotion and demotion of Content 113 to the Secondary Content sites is done periodically based on customer demand for the individual pieces of Content 113.

Content Hosting Router

[0258] The Content Hosting Router (not shown) resides in the Content Hosting Site(s) 111 and receives all requests from End-User(s) wanting to download Content 113. It performs validation checks on the End-User(s) request to ensure they indeed bought the Content 113. A database is maintained on the status of the Secondary Content Sites that includes what Content 113 is on them and their current status. This current status includes the amount of activity on the sites and whether a site is down for maintenance.

[0259] The only interface to the Content Hosting Router is the License SC(s) 660 that is sent by the End-User Device 109 when Content 113 is requested to be downloaded. The License SC(s) 660 includes information that indicates the user is allowed to download the Content 113.

Secondary Content Sites

[0260] The Secondary Content Sites (not shown) host the popular Content 113 of the Secure Digital Content Distribution System 100. These sites are geographically dispersed across the world and are located near Network Access Points (NAPs) to improve download times. These sites are added to the system as demand on the primary Content Hosting Site(s) 111 nears maximum capacity.

IX. ELECTRONIC DIGITAL CONTENT STORE(S)

A. Overview - Support for Multiple Electronic Digital Content Store(s) 103

[0261] Electronic Digital Content Store(s) 103 are essentially the retailers. They are the entities who market the Content 113 to be distributed to the customer. For distribution of Content 113, this would include Digital Content Retailing Web Site, Digital Content Retail Stores, or any business who wishes to get involved in marketing electronic Content 113 to consumers. These businesses can market the sale of electronic Content 113, gift or can choose to just add the Content 113 to their store. These businesses can offer for sale, introduction of downloadable electronic goods into the service offering of the Electronic Digital Content Store(s) 103 is accomplished via a set of tools developed for the Electronic Digital Content Store(s) 103 as part of the Secure Digital Content Electronic Distribution System 100.

[0262] These tools are used by the Electronic Digital Content Store(s) 103 to:

- acquire the Metadata SC(s) 620 packaged by the Content Provider(s) 101
- extract Content 113 from these SC(s) to be used as input to building their service offering
- create Offer SC(s) 641 describing the downloadable Content 113 they are offering for sale
- handle the acknowledgement of the sale and initiation of the download by creating and sending Transaction SC(s) 640 to the End-User Device(s) 108
- manage a transaction log of downloadable Content 113 and the status of each download
- handle status notifications and transaction authentication requests
- perform account reconciliation

[0263] The tools are designed to allow flexibility in how the Electronic Digital Content Store(s) 103 wishes to integrate

sale of downloadable electronic Content 113 into its service. This tool can be used in such a way as to request that all financial settlements for downloadable Content 113 purchased be handled by the Clearinghouse(s) 105 although this is not required. These tools also enable Electronic Digital Content Store(s) 103 to completely service their customers and handle the financial transactions themselves, including providing promotions and special offers. The tools enable the Electronic Digital Content Store(s) 103 is not required to host the downloadable Content 113 into its existing services. In addition, the Electronic Digital Content Store(s) 103 is not required to manage its Content 113 and does not have to manage its dissemination. This function is performed by the Content Hosting Site(s) 111 selected by the Content Provider(s) 101.

[0264] The tools for the Electronic Digital Content Store(s) 103 are implemented in Java in the preferred embodiment but other programming languages such as C/C++, Assembler and equivalent can be used. It should be understood that the tools described below for the Electronic Digital Content Store(s) 103 can run on a variety of hardware and software platforms. The Electronic Digital Content Store(s) 103 as a complete system or as any of its constituent components may be distributed as an application program in a computer readable medium including but not limited to electronic distribution such as the web or on floppy diskettes, CD ROMs and removable hard disk drives.

[0265] In another embodiment, the components of the Electronic Digital Content Store(s) 103 is part of a programmatic software toolkit. This toolkit enables predefined interfaces to the components of the generic Electronic Digital Content Store(s) 103 components and tools discussed below. These predefined interfaces are in the form of APIs or Application Programming Interfaces. A developer using these APIs can implement any of the functionality of the components from a high level application program. By providing APIs to these components, a programmer can quickly develop a customized Electronic Digital Content Store(s) 103 without the need to re-create these functions and resources of any of these components.

[0266] Electronic Digital Content Store(s) 103 are not limited to Web based service offerings. The tools provided are used by all Electronic Digital Content Store(s) 103 wishing to sell downloadable electronic Content 113 regardless of the transmission infrastructure or delivery mode used to deliver the Content 113 to End-User(s). Broadcast services offered over satellite and cable infrastructure also use these same tools to acquire, package, and track electronic Content 113 sales. The presentation of electronic merchandise for sale and the method in which these offers are delivered to the End-User(s) is the main variant between the broadcast based service offering and the point-to-point interactive web service type offering.

25 30 **B. Point-to-Point Electronic Digital Content Distribution Service**

[0267] Point-to-Point primarily means a one-to-one interactive service between the Electronic Digital Content Store(s) 103 and the End-User Device(s) 100. This typically represents an internet web based service provided via telephone or cable modem connection. Networks other than the Internet are supported in this model as well, as long as they conform to the Web Server/Client/Browser model. FIG. 9 is a block diagram illustrating the major tools, components and processes of an Electronic Digital Content Store(s) 103.

1. Integration Requirements

[0268] The Secure Digital Content Electronic Distribution System 100 not only creates new online businesses but provides a method for existing businesses to integrate the sale of downloadable electronic Content 113 to their current inventory. The suite of tools provided to the Electronic Digital Content Store(s) 103 simplify this integration effort. The Content Integration Tool 171 and the Packer Tool 153 provides a method for the Electronic Digital Content Store(s) 103 to acquire information from the participating Content Provider(s) 101 on what they have available for sale and to create the item required to reference these downloadable objects as items in their own inventory. This process is batch driven and can be largely automated and is executed only to integrate new Content 113 into the site.

[0269] The tools for the Secure Digital Content Electronic Distribution have been designed to allow integration of electronic downloadable Content 113 into typical implementations of web based Electronic Digital Content Store(s) 103 (i.e., Columbia House online, Music Boulevard, Q Tower) and equivalent with minimal change to their current Content 113 retailing paradigm. Several methods of integration are possible and in the preferred embodiment, the Electronic Digital Content Store(s) 103 provides support for all product searches, previews, selections (shopping cart), and purchases. Each Electronic Digital Content Store(s) 103 establishes customer loyalty with its customers and continues to offer its own incentives and market its products as it does today. In the Secure Digital Content Electronic Distribution System 100, it would simply need to indicate which products in its inventory are also available for electronic download and allow its customers to select the electronic download option when making a purchase selection. In another embodiment, the customer's shopping cart could contain a mixture of electronic (Content 113) and physical media selections. After the customer checks out, and the Electronic Digital Content Store(s) 103 has completed the financial settlement and logged or notified its shipping and handling functions to process the physical merchandise

purchased, the commerce handling function of the Electronic Digital Content Store(s) 103 then calls the Transaction Processor Module 175 to handle all electronic downloads. It simply passes the required information and all processing from that point on is handled by the tools for the Secure Digital Content Electronic Distribution System 100. In another embodiment, other methods of transaction handling are also possible using tools for the Secure Digital Content Electronic Distribution System 100 to handle the financial settlement should the Electronic Digital Content Store(s) 103 wish to sell downloadable merchandise only or to segregate the financial settlement of physical and downloadable merchandise.

[0270] To handle the downloading of merchandise, the Electronic Digital Content Store(s) 103 is given a Product ID (not shown) for each downloadable product that it acquires from the Content Promotions Web Site 159 for the Content Provider(s) 101. This Product ID is associated to a customer's purchase transaction to the downloadable product. The Product ID is what the Electronic Digital Content Store(s) 103 passes to the Transaction Processor Module 175 to identify the product that the user has purchased. The SC(s) (Offer/SC(s) 841) that were created to describe the products are loaded from the Electronic Digital Content Store(s) 103 and kept in an Offer Database 181 in an effort to simplify management of these objects and make their existence transparent to the Electronic Digital Content Store(s) 103.

[0271] The Transaction Processor Module 175 and other additional functions are provided as web server side executable (i.e., CGI and NSAPI, SAPi) callable functions or simply API's into a DLL or C object library. These functions handle run time processing for End-User(s) interactions and optional interactions with the Clearinghouse(s) 105. These functions interact with the web server's commerce services to create and download to the End-User Device(s) 100 the files necessary to initiate the Content 113 download process. They also handle optional interactions to provide authorizations and accept notifications of completion of activities.

[0272] An Accounting Reconciliation Tool 178 is also provided to assist the Electronic Digital Content Store(s) 103 in conducting the Clearinghouse(s) 105 to reconcile accounts based on its own and the transaction logs of the Clearinghouse(s) 105.

2. Content Acquisition Tool 171

[0273] The Content Acquisition Tool 171 is responsible for interfacing with the Content Promotions Web Site 158 to preview and download Metadata SC(s) 620. Since the Content Promotions site is a standard web site, a web browser is used to display the Electronic Digital Content Store(s) 103 to navigate the site. The navigation features varies based on the site design of the Content Provider(s) 101. Some sites may provide extensive search capabilities with many screens to select from. All sites include the selection of Metadata SC(s) 620 containing all the promotional and descriptive information of a song or album.

[0274] Alternatively, the Electronic Store(s) 103 may subscribe to content updates and receive updates automatically via FTP.

Viewing Metadata

[0275] The Content Acquisition Tool 171 is a web browser helper application which launches whenever a Metadata SC(s) 620 (not selected at the Content Promotions Web Site 158) Selection of the SC(s) causes it to be downloaded to the Electronic Digital Content Store(s) 103, and launch the helper application. The Content Acquisition Tool 171 opens the Metadata SC(s) 620 and display the non-encrypted information contained therein. Displayed information includes Extracted Metadata 173 for a music example, the graphic image(s) associated with the song and the information describing the song, a preview clip of the song can also be listened to if included in the Metadata SC(s) 620.

[0276] In an example where the Content 113 is music, promotional information about the song or album, the album title, and the artist is also shown if provided by the Content Provider(s) 101. This information is displayed as a series of linked HTML pages in the browser window. Purchasable Content 113 such as the song and the lyrics and whatever other metadata the Content Provider(s) 101 wishes to protect, is not accessible to the Retail Content Web Site 180.

[0277] In another embodiment, the Content Provider(s) 101 provides optional promotional content for a fee. In this embodiment such promotional content is encrypted in the Metadata SC(s) 620. Financial settlement to open this data can be handled via the Clearinghouse(s) 105 with the account for the Electronic Digital Content Store(s) 103 being charged the designated fee.

Extracting Metadata

[0278] Besides the preview capabilities, this tool provides two additional features: metadata extraction and preparation of an Offer SC(s) 641. Selection of the metadata extraction option prompts the Electronic Digital Content Store(s) 103 to enter the path and filenames to where the metadata is to be stored. Binary metadata such as graphics and

the audio preview clip is stored as a separate file. Text metadata is stored in an ASCII delimited text file which the Retail Content Web Site 150 can then import into its database. A table describing the layout of the ASCII delimited file is also be created in a separate TOC file. Additional options is available to allow extraction into other National Languages Support (NLS) supported formats.

[0278] One important piece of information provided in the extracted data is the Product ID. This Product ID is what the commerce handling function for the Electronic Digital Content Store(s) 103 needs to identify to the Transaction Processor Module 175 (for more information, refer to Transaction Processing section). The Content 113 that the user has purchased. The Transaction Processor Module 175 uses this Product ID to properly retrieve the appropriate Offer SC(s) 641 from the Offer Database 181 for subsequent download to the End-User Device(s) 109. The Electronic Digital Content Store(s) 103 has full control over how it presents the offer of downloadable Content 113 on its site. It only needs to make a cross reference of the Content 113 being offered to this Product ID to properly interface with the tools for the Secure Digital Content Electronic Distribution System 100, providing this information here, allows the Electronic Digital Content Store(s) 103 to integrate this product or Content 113 into its inventory and sales pages (database) in parallel with the Offer SC(s) 641 creation process since both processes uses the same Product ID to reference the product. This is described further below.

Offer SC(s) Creation Packer 153

[0279] The Electronic Digital Content Store(s) 103 is required to create an Offer SC(s) 641 describing the downloadable Content 113 that is for sale. Most of the information that goes into the Offer SC(s) 641 is derived from the Metadata SC(s) 620. The Content Acquisition Tool 171 creates the Offer SC(s) 641 by:

- prompting parts from the Metadata SC(s) 620 that are not required to be included in the Offer SC(s) 641 as defined by the Offer SC(s) Template in the Metadata SC(s) 620
- adding additional required parts as defined by default specified by the configuration options in this tool for the Electronic Digital Content Store(s) 103
- prompting for additional required inputs or selections as defined by the Offer SC(s) Template in the Metadata SC(s) 620

calling the SC(s) Packer 153 to pack this information into the SC(s) format

[0280] Metadata to be displayed by the Player Application 185 (further described later) on the End-User Device(s) 109 is kept in the Metadata SC(s) 620. Other promotional metadata that was only used by the Electronic Digital Content Store(s) 103 as input to its web service database is removed from the Metadata SC(s) 620. Right management information provided by the Content Provider(s) 101, such as watermarking instructions, encrypted Symmetric Keys 622, and Usage Conditions 517 defining the permitted uses of the object, are also retained.

[0281] This stripped down Metadata SC(s) 620 is then included in the Offer SC(s) 641. The Electronic Digital Content Store(s) 103 also attaches its own Usage Conditions called Store Usage Conditions 519 or purchase options to the Offer SC(s) 641. This can be accomplished interactively or automatically through a set of defaults. If configured to be processed interactively, the Electronic Digital Content Store(s) 103 is prompted with the set of permitted object Usage Conditions 517 as defined by the Content Provider(s) 101. He then selects the option(s) he wishes to offer to his customers. These now become the new Usage Conditions or Store Usage Conditions 519. To process automatically, the Electronic Digital Content Store(s) 103 constructs a set of default purchase options to be offered for all Content 113. These default options are automatically checked against the permitted Usage Conditions 517 defined by the Content Provider(s) 101 and is set in the Offer SC(s) 641 if there are no discrepancies.

[0282] Once the Offer SC(s) 641 is created, it is stored in an Offer Database 181 and is indexed with the Product ID pre-assigned in the Metadata SC(s) 620. This Product ID is used later by the Electronic Digital Content Store(s) 103 to identify the downloadable Content 113 being purchased by a customer when interfacing with the Offer Database 181 to retrieve the Offer SC(s) 641 for packaging and transmission to the End-User(s). See the Transaction Processor Module 175 section for more details.

[0283] In another embodiment, the Electronic Digital Content Store(s) 103 hosts the Content SC(s) 641 at its site. This embodiment requires changes to the Offer SC(s) 641 such as the replacement of the URL of the Content Hosting Site(s) 111 with the URL of the Electronic Digital Content Store(s) 103.

3. Transaction Processing Module 175

[0284] Electronic Digital Content Store(s) 103 directs billing to Clearinghouse(s) 105. Alternatively, the Electronic Digital Content Store(s) 103 may request financial clearance direct from the Clearinghouse(s) 105. There are two basic modes for processing End-User(s) purchase requests for downloadable Content 113. If the Electronic Digital Content

Store(s) 103 does not wish to handle the financial settlement of the purchase and has no special promotions or incentive governing the sale of the merchandise and does not use a shopping cart metaphor for batching the purchase requests. It may opt to provide links on its Content 113 download page directly to the Offer SC(s) 641 files. These Offer SC(s) 641 would have to have been built with retail pricing information included in the metadata. Also included in the Offer SC(s) 641 is a special HTML offer page containing the purchase options with terms and conditions of the sale. This page is built from a template created when the Offer SC(s) 641 was built. When the End-User(s) clicks on the direct link to the Offer SC(s) 641, the Offer SC(s) 641 is downloaded to the browser End-User Device(s) 109 launching a helper application which opens the container and present the offer page included in the Offer SC(s) 641. This page contains a form to collect customer information including credit card information and purchase option selection. The form then gets submitted directly to the Clearinghouse(s) 105 for financial settlement and processing. Obviously, this form may contain the fields needed to use the End-User(s) credit information or industry standard local transaction handler.

[0285] An embodiment where the Electronic Digital Content Store(s) 103 handles billing is now described. The more typical mode of handling purchase requests is to allow the Electronic Digital Content Store(s) 103 to process the financial settlement and then submit the download authorization to the End-User(s). This method allows the Electronic Digital Content Store(s) 103 to integrate with other merchandise offered for sale in this environment, the offer of downloadable Content 113 is included in this shopping pages which get added to a shopping cart when selected by the End-User(s) and get processed and financially settled as is done in the Electronic Digital Content Store(s) 103 current shopping model. Once the financial settlement is completed, the commerce handling process of the Electronic Digital Content Store(s) 103 then calls the Transaction Processor Module 175 to complete the transaction.

Transaction Processor Module 175

[0286] The role of the Transaction Processor Module 175 is to put together the information needed by the End-User Device(s) 109 to initiate and process the download of the Content 113 purchased. This information is packaged into a Transaction SC(s) 640 which is sent back to the End-User Device(s) 109 by the Web Server as the response to the purchase submission. The Transaction Processor Module 175 requires three pieces of information from the commerce handling process of the Electronic Digital Content Store(s) 103: the Product IDs for the Content 113 purchased, Transaction Data 642, and an HTML page or CGI URL acknowledging the purchase settlement.

[0287] The Product ID is the value provided in the Transaction Data 642 in the Metadata SC(s) 620 associated to the Content 113 just sold. This Product ID is used to retrieve the associated Offer SC(s) 641 from the Offer Database 181.

[0288] The Transaction Data 642 is a structure of information provided by the transaction processing function of the Electronic Digital Content Store(s) 103 which is later used to correlate the Clearinghouse(s) 105 processing with the financial settlement transaction performed by the Electronic Digital Content Store(s) 103 and to provide user identity information to be included in the watermark of the Content 113 downloaded to the End-User Device(s) 109. When the Clearinghouse(s) 105 receives a valid Offer SC(s) 650, it logs a transaction indicating the Content 113 that was sold, which Electronic Digital Content Store(s) 103 sold it and the associated Transaction Data 642 including the End-User Name and ID Transaction ID 535. The Transaction ID 535 provides a reference to the financial settlement transaction. This information is later returned by the Clearinghouse(s) 105 to the Electronic Digital Content Store(s) 103 for use in recording its account with the billing statements received from the Content Provider(s) 101 (or his agent). The Clearinghouse Transaction Log 178 can be used by the Content Provider(s) 101 to determine what Content 113 of his has been sold and enables him to create a bill to each Electronic Digital Content Store(s) 103 for royalties owed him. Other electronic means besides billing can alternatively be used to settle accounts between the Content Provider(s) 101 and Electronic Digital Content Store(s) 103.

[0289] The information provided in the Transaction SC(s) 640 and the security and integrity of the Transaction SC(s) 640 provide sufficient authenticity to the Clearinghouse(s) 105 that the purchase transaction is valid and thus no further validation is required prior to the logging of this sale by the Clearinghouse(s) 105. The Electronic Digital Content Store(s) 103, however, has the option to request authentication before its accounts are charged (transaction logged at the Clearinghouse(s) 105 indicating to the Content Provider(s) 101 that the Electronic Digital Content Store(s) 103 has collected money for the sale of this Content 113). This request for authentication/verification is indicated by a tag in the Transaction Data 642. In this scenario, the Clearinghouse(s) 105 contacts the Electronic Digital Content Store(s) 103 and receive a authorization from the Electronic Digital Content Store(s) 103 before the charge to its account and the release of the encryption Key 623. The Transaction ID 535 is passed to the Electronic Digital Content Store(s) 103

from the Clearinghouse(s) 105 as part of the authentication request to enable the Electronic Digital Content Store(s) 103 to associate this request to a prior transaction performed with the End-User(s). This Transaction ID 535 can be any unique value the Electronic Digital Content Store(s) 103 wishes to use and is solely for its benefit.

[0280] The Transaction Data 642 also contains a customer's name. This name can be from the user name field of the purchase form filled out by the user when making his purchase, or from information logged previously during some user registration process with the Electronic Digital Content Store(s) 103, or the circuit name obtained from credit card information associated with the card used in this transaction. This name is later included in the License Watermark 527.

[0281] The Transaction Data 642 also contains the Store Usage Conditions 519 purchased by the End-User(s). This information is included in the License Watermark 527 and used by the End-User Device(s) 109 in Copy and Play Control.

[0282] The final parameter required by the Transaction Processor Module 175 is the HTML page or CGI URL acknowledging the purchase settlement. The purpose of this is to allow the Electronic Digital Content Store(s) 103 to respond to the End-User(s) with an acknowledgement of the financial settlement and whatever other information he wishes to include in the response. This HTML page or CGI URL is included in the Transaction SC(s) 640 and displayed in the browser window of the End-User Device(s) 109 when the Transaction SC(s) 640 is received and processed.

[0283] The Transaction SC(s) 640 is the HTML response to the End-User(s) from the Electronic Digital Content Store(s) 103 after processing the purchase submission. Sending a SC(s) as the direct HTTP response forces the automatic loading on the End-User Device(s) 109 of a SC(s) Processor Helper Application thus allowing automatic completion of the transaction without depending on further End-User(s) initiated actions. This process is described in more detail in the End-User Device(s) 109 and Player Application section later.

[0284] When the Transaction Processor Module 175 is called with the required parameters, it builds a Transaction SC(s) 640 containing the Transaction Data 642, the transaction acknowledgement HTML page or reference URL, other required security features of the SC(s), and retrieves the Offer SC(s) 641 associated with the purchase. It also logs information about this transaction for later use by the Notification Interface Module 176 and the Account Recconciliation Tool 178.

4. Notification Interface Module 176

[0285] The Notification Interface Module 176 is a Web Server side executable routine (CGI or function callable by NSAPI, ISAPI or equivalent). It handles optional requests and notifications from the Clearinghouse(s) 105, the End-User Device(s) 109, the Content Hosting Site(s) 111, and the Content Provider(s) 101. The events that the Electronic Digital Content Store(s) 103 can optionally request notification for are:

[0286] Notification from the Clearinghouse(s) 105 that the End-User Device(s) 109 requested an encryption Key 623 and the Clearinghouse(s) 105 is releasing the encryption Key 623 for the specified Content 113. This notification can optionally be configured to require authentication from the Electronic Digital Content Store(s) 103 prior to the encryption Key 623 being sent to the End-User Device(s) 109.

[0287] Notification from the Content Hosting Site(s) 111 that the Content SC(s) 630 has been sent to the End-User Device(s) 109.

[0288] Notification from the End-User Device(s) 109 that the Content SC(s) 630 and the License SC(s) 660 have been received and successfully used to purchase the Content 113 or was found to be corrupt.

[0289] Notification from the Content Provider(s) 101 that new Content 113 has been placed in the Content Promotions Web Site 158.

[0290] None of these notifications are a required step in the Secure Digital Content Electronic Distribution System

flows 100, but are provided as options to allow the Electronic Digital Content Store(s) 103 the opportunity to close its record on the satisfaction or completion of the sale. It also provides information that may be needed to handle customer service requests by letting the Electronic Digital Content Store(s) 103 know what functions have transpired since its financial settlement of the transaction, or what errors occurred during an attempt to complete the sale. Alternatively much of this status can be obtained from the Clearinghouse(s) 105 through the Customer Service Interface 164 as needed.

[0291] Frequency of notification of new Content 113 available at the Content Promotions Web Site 158 is determined by the Content Provider(s) 101. Notification may be provided as each new Metadata SC(s) 620 is added or just daily with all new Metadata SC(s) 620 added that day.

[0292] All of these notifications result in entries being made to the Transaction Log 176. If the Electronic Digital Content Store(s) 103 wishes to perform his own processing on these notifications, he can intercept the CGI call, perform his unique function and then optionally pass the request on to the Notification Interface Module 176.

5. Account Reconciliation Tool 178

[0293] This Account Reconciliation Tool 178 contacts the Clearinghouse(s) 105 to compare the Transaction Log 176 with the log of the Clearinghouse(s) 105. This is an optional process which is available to help the Electronic Digital Content Store(s) 103 feel comfortable with the accounting for the Secure Digital Content Distribution System 100.

[0294] In another embodiment, this tool can be updated to provide electronic funds transfers for automated periodic payments to the Content Provider(s) 101 and the Clearinghouse(s) 105 after recording the bill against the user's payments upon receipt of an electronic bill from the Clearinghouse(s) 105 after recording the bill against the Transaction Log 176.

C. Broadcast Electronic Digital Content Distribution Service

[0295] Broadcast primarily refers to a one to many transmission method where there is no personal interaction between the End-User Device(s) 109 and the Electronic Digital Content Store(s) 103 to customize on-demand viewing and listening. This is typically provided over a digital satellite or cable infrastructure where the Content 113 is programmed so that all End-User Device(s) 109 receive the same stream.

[0296] A hybrid model can also be defined such that an Electronic Digital Content Store(s) 103 provides a digital content service organized in such a way that it can offer both a web distribution interface via an Internet connection as well as a higher bandwidth satellite or cable distribution interface via a broadcast service, with a great deal of commonly to the site design. If the IRD broadcast serial interface were connected to the web, and the IRD-supported web navigation, the End-User Device(s) could navigate the Content 113 to purchase. The user can select high quality downloadable Content 113, purchase these selections, and receive the required license SC(s) 650 all via an Internet connection and then request delivery of the Content 113 (Content SC(s) 630) over the higher bandwidth broadcast interface. The Web service can indicate which Content 113 would be available for download. In this manner based on the broadcast schedule or could build the broadcast streams based totally on purchased Content 113. This method would allow a Web based digital content service to contract with a broadcast facility to deliver high quality Content 113 to users equipped with this manner and the extra catalog available for download in lower quality via the web interface.

[0297] Other broadcast models can be designed when there is no web interface to the End-User Device(s) 109. In this model, promotional content is packaged in specially digital streams for broadcast delivery to the End-User Device(s) 109 (a.k.a. IRD) where special processing is performed to decode the streams and present the End-User with the promotional content from which purchase selection can be made.

[0298] The actual purchase selections would still be initiated via backchannel communications from the End-User Device(s) 109 to the Clearinghouse(s) 105 and would utilize SC(s) to perform all data exchange. The toolset provided to the Electronic Digital Content Store(s) 103 has been architected and developed in such a way that most of the tools apply to both a point-to-point Internet service offering as well as a broadcast satellite or cable offering. The tools used by a Digital Content Web Site Electronic Digital Content Store(s) 103 to acquire and manage Content 113 as well as prepare SC(s) is also used by a satellite based Electronic Digital Content Store(s) 103 to manage and prepare Content 113 for distribution on a broadcast infrastructure. The SC(s) distributed over a Web service are the same as those distributed over a broadcast service.

X. END-USER DEVICE(s) 109

[0299] The applications in the End-User Device(s) 109 for the Secure Digital Content Electronic Distribution System 100 perform two main functions: first the SC(s) processing and copy control; and second playback of encrypted Content 113. Whether the End-User Device(s) 109 is a Personal Computer or a specialized electronic consumer device, it has to be capable of performing these two functions. The End-User Device(s) 109 also provides a variety of additional features and functions like creating play lists, managing the digital content library, displaying information and images during content playback, and recording to external media devices. These functions are very based on the services these applications are supporting and the type of device the applications are designed for.

A. Overview

[0300] Referring now to FIG. 10, shown is the major components and processes and End-User Device(s) 109 Functional Flow. The applications designed to support a PC based web interface Content 113 service consists of two executable software applications: the SC(s) Processor 192 and the Player Application 195. The SC(s) Processor 192 is

an executable application which is configured as a Helper Application into the End-User(s) Web Browser 191 to handle SC(s) File/MIME Types. This application is launched by the Browser whenever SC(s) are received from the Electronic Digital Content Store(s) 103, the Clearinghouse(s) 105, and the Content Hosting Site(s) 111. It is responsible for performing all required processing of the SC(s) and eventually adding Content 113 to the Digital Content Library 198 of the End-User(s).

[0307] The Player Application 195 is a stand alone executable application which the End-User(s) loads to perform Content 113 in the Digital Content Library 198, manage his Digital Content Library 198 and create copies of the Content 113 if permitted. Both the Player Application 195 and SC(s) Processor 192 applications can be written in Java, C/C++ or any equivalent software. In its preferred embodiment, the applications can be downloaded from computer readable means such as website. However, other delivery mechanisms are also possible such as being delivered on computer readable media such as diskettes or CDs.

[0308] The searching and browsing of Content 113 information, previewing of, for example, song clips, and selecting songs for purchase is all handled via the End-User(s) Web Browser 191. Electronic Digital Content Store(s) 103 provides the shopping experience in the same way that is offered today by many Content 113 retailing web sites. The difference to the End-User(s) over today's web based Content 113 shopping is that they may now select downloadable Content 113 objects to be added to their shopping cart. If the Electronic Digital Content Store(s) 103 has other merchandise available for sale in addition to the downloadable objects, the End-User(s) may have a combination of physical and electronic downloadable merchandise in the shopping cart. The Secure Digital Content Electronic Distribution End-User Device(s) 108 are not involved until after the End-User(s) checks out and submits his final purchase authorization to the Electronic Digital Content Store(s) 103. Prior to this point, all interaction is between the Web Server for the Electronic Digital Content Store(s) 103 and the Browser 191 on the End-User Device(s) 108. This includes preview of sample Digital Content clips. Digital Content clips are not packaged into SC(s) but instead are integrated into the web service of the Electronic Digital Content Store(s) 103 as downloadable file or sent from a streaming server. The format of the Content 113 clip is not dictated by the system architecture. In another embodiment, the Player Application 195 could interact directly with the Electronic Digital Content Store(s) 103 or Clearinghouse(s) 105 or online using a promotional CD.

B. Application Installation

[0309] The Player Application 195 and the Helper Application 1981 are packaged into a self installing executable program which is available for download from many web sites. The Clearinghouse(s) 105 acts as a central location which hosts the master download page at a public web site. It contains links to the locations from which the installation package can be downloaded. The installation package is available at all Content Hosting Site(s) 111 to provide geographic dispersion of the download requests. Each participating Electronic Digital Content Store(s) 103 can also make the package available for download from their site or may just provide a link to the master download page at the public web site of the Clearinghouse(s) 105.

[0310] Any End-User(s) wishing to purchase downloadable Content 113, downloads and installs this package. The installation is self contained in this downloadable package. It unpacks and installs both the Helper Application 198 and the Player Application 195 and also configures the Helper Application 198 to the installed Web Browser(s).

[0311] As part of the installation, a Public/Private Key 881 pair is created for the End-User Device(s) 109. This pair is used in the package available for download from their site or may just provide a link to the master download page at the public web site of the Clearinghouse(s) 105.

[0312] Any End-User(s) wishing to purchase downloadable Content 113, downloads and installs both the Helper Application 198 and the Player Application 195 and also configures the Helper Application 198 to the installed Web Browser(s).

[0313] One type of tamper-resistant software technology is from IBM. One product this code was introduced is in the IBM ThinkPad 770 laptop computer. Here, the tamper-resistant software was used to protect the DVD movie player in the computer. Digital Content Provider(s) such as Hollywood studios, concerned about the advent of digital movies and the ease at which perfect copies can be made, have patented the movies on DVD disc(s) contain copy protection mechanisms. IBM's tamper-resistant software made it difficult to circumvent these copy protection mechanisms. This

is a very typical application for tamper-resistant software; the software is used to enforce rules on the usage of some protected type of Content 113.

[0314] IBM's tamper-resistant software puts several types of obstacles in the path of the attacker. First, it contains techniques to detect, or at least reduce the effectiveness of, the standard software tools that the hacker uses; debuggers and disassemblers. Second, it contains self integrity checking, so that single modifications, or even small handfuls of modifications, will be detected and cause incorrect operation. Finally, it contains obfuscations to mislead hackers regarding its use operation. The latter technique is largely ad hoc, but the first two build upon well-known tools in cryptography, encryption and digital signatures.

C. Secure Container Processor 192

[0315] When the End-User(s) submits the final purchase authorization to the Electronic Digital Content Store(s) 103 for the merchandise he has selected in his shopping cart, his Web Browser remains active waiting for a response from the Web Server. The Web Server at the Electronic Digital Content Store(s) 103 processes the purchase and performs the financial settlement and then returns a Transaction SC(s) 640 to the End-User Device(s) 109. The SC(s) Processor 192 (Helper Application 198) is launched by the Web Browser to process the SC(s) into type associated with the Transaction SC(s) 640. FIG. 14 is an example of user interface screens of the Player Application 195 downloading content to a local library as described in FIG. 10 according to the present invention.

[0316] The SC(s) Processor 192 opens the Transaction SC(s) 640 and extracts the Response HTML page and Offer SC(s) 641 contained within. The Response HTML page is displayed in the Browser window acknowledging the End-User(s) purchase. The Offer SC(s) 640 are then opened and the Content 113 (e.g. song or album) names along with the projected download times are extracted from them. Step 1401. A new window 139 is then displayed with this information and the End-User(s) is presented with options to schedule the download(s) of the Content 113 (e.g. for music, songs or entire albums); step 1402. The End-User(s) can select immediate download or can schedule the download to occur at a later time. If a later time is selected, the download schedule information is saved in a log and the download is initiated at the scheduled time if the End-User Device(s) 109 is powered on at that time. If the computer is not active at the scheduled download time or the communication link is not active, the End-User(s) is prompted to reschedule the download when the computer is next powered up.

[0317] When the scheduled download time occurs or if immediate download was requested, the SC(s) Processor 192 creates Offer SC(s) 650 from information in the Transaction SC(s) 640, Offer SC(s) 641, and the Public Key 861 of the End-User(s) generated at initial time. This Offer SC(s) 650 is sent via HTTP request to the Clearinghouse(s) 105. When the Clearinghouse(s) 105 returns the License SC(s) 860, the Helper Application 198 is re-invoked to process the License SC(s) 860. The License SC(s) 860 is then opened and the URL of the Content Hosting Site(s) 111 is extracted from the referenced Offer SC(s) 650. The License SC(s) 860 is then sent to the specified Content Hosting Site 111, via http request through the Browser. The download of the Content SC(s) 650. When the Content SC(s) 650 comes back to the Browser, the Helper Application 198 is re-invoked again. The SC(s) Processor 192 displays the name of the Content 113 being downloaded along with a download progress indicator and an estimated time to completion.

[0318] As the Content 113 is being received by the SC(s) Processor 192, it loads the Content 113 data into memory buffers for decryption. The size of the buffers depends on the requirements of the encryption algorithm and watermarking technology 193 and is the minimum size possible to reduce the amount of unencrypted Content 113 exposed to the hacker code. As a buffer is full, it is decrypted using the Key 822 (corresponding to the Public Key 861) of the End-User(s) extracted from the License SC(s) 860, which itself is first decrypted using the Private Key 861 of the End-User(s) is then passed to the watermarking function.

[0319] The watermarking 193 extracts the watermarking instructions from the License SC(s) 860 and decrypt the instructions using the Private Key of the End-User(s). The watermarking data is then extracted from the License SC(s) 860 which includes transmission information such as the purchaser's name as registered with the Electronic Digital Content Store(s) 103 from which the Content 113 was purchased or derived from the credit card registration information. If the Electronic Digital Content Store(s) 103 does not provide a registration function, also included in the watermark is the purchase date and the Transaction ID 538 assigned by the Electronic Digital Content Store(s) 103 to reference the specific records logged for this transaction. The Store Usage Conditions 518 are also included to be used by the Copy Control of the Player Application 195.

[0320] The Watermarking 193 is protected with Tamper Resistant Code technology so as not to divulge the watermark instructions thus preventing a hacker from discovering the location and technique of the watermark. This prevents removal or modification of the watermark by a hacker.

[0321] After inserting any required watermark to this content buffer, the buffer is passed to the scrambling function for Re-Encryption 194. A processor efficient secure encryption algorithm such as IBM's SEAL encryption technology is used to re-encrypt the Content 113 using a random Symmetric Key. Once the download and Decryption and Re-

Encryption 194 process is complete, the encryption Key 623 used by the Content Provider(s) 101 to originally encrypt the Content 113 is now destroyed and the new SEAL key is itself encrypted using the Secret User Key created and hidden at installation time. The new encrypted Seal Key is now stored in the License Database 107.

[0322] Unlike source performed at the Content Provider(s) 101 and user watermarking performed at the End User Device(s) 109 may need to become an industry standard to be effective. These standards are still evolving. The technology is available to allow control information to be embedded in the music and updated a number of times. Until such time as the copy control standards are more stable, alternative methods of copy control have been provided in the Secure Digital Content Electronic Distribution System 100 so that it does not rely on the copy control watermark in order to provide rights management in the consumer device. Storage and playback usage conditions security is implemented utilizing encrypted DC Library Collections 196 that are tied to the End User Device(s) 109 and protected via the Tamper Resistant Environment. Software hooks are in place to support copy control watermarking when standards have been adopted. Support exists today for watermarking AAC and other encoded audio streams at a variety of compression levels but the technology is still somewhat immature at this time to be put to use as a sole method of copy control.

[0323] The Decryption and Re-Encryption 194 process is another area of the code that is protected with Tamper Resistant Code technology so as not to divulge the original Content 113 encryption key, the new SEAL key, the Secret User Key, and where the Secret User Key segments are stored and how the key is segmented.

[0324] The process of Decryption and Re-Encryption 194 serves two purposes. Storing the Content 113 encrypted with an algorithm like SEAL enables faster than real-time decryption and requires much less processor utilization to perform the decryption than does a more industry standard type algorithm like DES. This enables the Player Application 195 to perform a real-time concurrent decryption-decode-playback of the Content 113 without the need to first decrypt the entire file for the Content 113 prior to decode and playback. The efficiency of the SEAL algorithm and a highly efficient decode algorithm, allows not only concurrent operation, streamlining playback from the encrypted file but also allows this process to occur on a much lower powered system processor. Thus this application can be supported on a End-User Device(s) 109 as low end as a 60MHz Pentium system and perhaps lower. Separating the encryption selection of the original content encryption algorithm. Thus use of widely accepted and proven industry standard algorithms can be used thus further enhancing Digital Content industry acceptance of the Secure Digital Content Electronic Distribution System 100.

[0325] The second purpose of this Decryption and Re-Encryption 194 process is to remove the requirement that the original master encryption Key 623, used by the Content Provider(s) 101 to encrypt this Content 113, be stored on every End-User Device(s) 109 which has licensed this Content 113. The encrypted master Key 623, as part of the License SC(e) 660, is only cached on the hard disk of the End-User Device(s) 109 for a very short time and is in the clear only in memory and for a very short time. During the execution phase, the Key 623 is protected via Tamper Resistant Code technology. Not having to retain this Key 623 in any form on the End-User Device(s) 109 once this Decryption and Re-Encryption 194 phase has completed, greatly lessens the possibility of piracy from hackers.

[0326] Once the song has been re-encrypted, it is stored in the Digital Content Library 196. All metadata required for use by the Player Application 195, is extracted from the associated Offer SC(e)s 641 and also stored in the Digital Content Library 196, step 1403. Any parts of the metadata which are encrypted, such as the song lyrics, are decrypted and re-encrypted in the same manner as described above for the other content. The same SEAL key used to encrypt the Content 113 is used for any associated metadata needing to be encrypted.

D. The Player Application 195

45 1. Overview

[0327] The Secure Digital Content Electronic Distribution Player Application 195 (referred to here as the Player Application 195) is analogous to both a CD, DVD or other Digital Content player and to a CD, DVD, or other digital content storage management system. At its simplest, it performs such as playing songs or video. At another level, it provides the End-User(s) 109 tool for managing their Digital Content Library 196. And just as importantly, it provides for selling and playing of collections of content, such as songs, (referred to here as Play-lists).

[0328] The Player Application 195 is assembled from a collection of components that may be individually selected and customized to the requirements of the Content Provider(s) 101 and Electronic Digital Content Store(s) 103. A generic version of the player is described, but customization is possible.

[0329] Referring now to FIG. 15 there is shown a block diagram of the major components and processes of the Player Application 195 running on End-User Device(s) 109 of FIG. 10.

[0330] There are several component-sets that make up the subsystems of the Player Object Manager 1501:

- 1. End-User Interface Components 1509
- 2. Copy/Play Management Components 1504
- 3. Decryption 1505, Decompression 1506, Playback Components 1507 and may include recording.
- 4. Data Management 1502 and Library Access Components 1503
- 5. Inter-application Communication Components 1508
- 6. Other miscellaneous (Installation, etc) Components

[0331] Components from within each of these sets may be selected, based on the requirements of:

- 10 - the platform (Windows, Unix, or equivalent)
- communications protocols (network, cable, etc)
- Content Provider(s) 101 or Electronic Digital Content Store(s) 103
- Hardware (CD, DVD, etc)
- Clearinghouse(s) 105 technology and more.

[0332] The sections below detail the various component sets. The final section details how these components are put together in the generic player, and discusses how the components can be customized.

[0333] In another embodiment, the components of the Player Application 195 and the SC(e) Processor 192 are available as part of a programmer's software toolkit. This toolkit enables predefined interfaces to the components of the generic player application listed above. These predefined interfaces are in the form of APIs or Application Programming Interfaces. A developer using these APIs can implement any of the functionality of the components from a high level application program. By providing APIs to these components, a programmer can quickly develop a customized Player Application 195 without the need to re-created these functions and resources of any of these components.

15 2. End-User Interface Components 1509

[0334] Components from this set combine to provide the on-screen manifestation of the Player Application 195. Note that the design establishes no definitive layout of these components. One such layout is provided in the generic player. Based on requirements from Content Provider(s) 101 and/or Electronic Digital Content Store(s) and other requirements, alternate layouts are possible.

[0335] This set is grouped into subgroups, starting with the components used to present End-User Display 1510 and media controls called End-User Controls 1511 used for such low-level functions as audio playback, and presentation of metadata. Next, the End-User Display Component 1510 is further divided by special function groupings (Play-list Digital Content Library), and then object-container components used for grouping and placing of those lower-level components.

[0336] Within the component listings below, any reference to creating CDs or copying of Content 113 to a CD or other recordable medium only applies to the case where the Player Application 195 has such functionally enabled. Also note that the term CD in that context is a generic one, that can also represent various other external recording devices, such as MiniDisc or DVD.

[0337] FIG. 16 is an example user interface screen of the Player Application 195 of FIG. 15 according to the present invention. Function for the End-User Controls 1511 include (corresponding screens of an End-User interface are shown 1601-1605):

[0338] Controls for performing the Content 113:

- 45 - Play/Stop button
- Play button
- Stop button
- Pause button
- Stop forward button
- Stop backward button
- Volume control
- Track position control/display
- Audio channel volume level display and more.

- [0339] Controls for the displaying metadata associated with the Content 113
- Cover Picture button
- Cover Picture object

- Artist Picture button
- Artist Picture object
- Track List button
- Track List Information object
- Track List Selector object (click to play)
- Track Name object
- Track Information object
- Track Lyric button
- Track Lyric object
- Track Artist Name object
- Track Credits button
- Track Credits object
- CD Name object
- CD Credits button
- CD Credits object
- Generic (Configurable) Metadata button
- Generic Metadata object and more.

- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28
- 29
- 30
- 31
- 32
- 33
- 34
- 35
- 36
- 37
- 38
- 39
- 40
- 41
- 42
- 43
- 44
- 45
- 46
- 47
- 48
- 49
- 50
- 51
- 52
- 53
- 54
- 55
- 56
- 57
- 58
- 59
- 60
- 61
- 62
- 63
- 64
- 65

- Artist Picture button
- Artist Picture object
- Track List button
- Track List Information object
- Track List Selector object (click to play)
- Track Name object
- Track Information object
- Track Lyric button
- Track Lyric object
- Track Artist Name object
- Track Credits button
- Track Credits object
- CD Name object
- CD Credits button
- CD Credits object
- Generic (Configurable) Metadata button
- Generic Metadata object and more.

[0340] Function for the End-User Display 1510 Include (corresponding screens of an End-User interface are shown 1601 - 1605):

[0341] Playlist of display container

- Play-List Management button
- Play-List Management window
- Digital Content search button
- Digital Content search Distribution object
- Digital Content search Submit button
- Copy Selected Search Results item To Play-List button
- Play-List object (relative)
- Play-List Save button
- Play-List Play button
- Play-List Pause button
- Play-List Restart button
- Create CD from Play-List button and more.

[0342] Display of Digital Content Library 198

- 40
- 41
- 42
- 43
- 44
- 45
- 46
- 47
- 48
- 49
- 50
- 51
- 52
- 53
- 54
- 55
- 56
- 57
- 58
- 59
- 60
- 61
- 62
- 63
- 64
- 65
- 66
- 67
- 68
- 69
- 70
- 71
- 72
- 73
- 74
- 75
- 76
- 77
- 78
- 79
- 80
- 81
- 82
- 83
- 84
- 85
- 86
- 87
- 88
- 89
- 90
- 91
- 92
- 93
- 94
- 95
- 96
- 97
- 98
- 99
- 100
- 101
- 102
- 103
- 104
- 105
- 106
- 107
- 108
- 109
- 110
- 111
- 112
- 113
- 114
- 115
- 116
- 117
- 118
- 119
- 120
- 121
- 122
- 123
- 124
- 125
- 126
- 127
- 128
- 129
- 130
- 131
- 132
- 133
- 134
- 135
- 136
- 137
- 138
- 139
- 140
- 141
- 142
- 143
- 144
- 145
- 146
- 147
- 148
- 149
- 150
- 151
- 152
- 153
- 154
- 155
- 156
- 157
- 158
- 159
- 160
- 161
- 162
- 163
- 164
- 165
- 166
- 167
- 168
- 169
- 170
- 171
- 172
- 173
- 174
- 175
- 176
- 177
- 178
- 179
- 180
- 181
- 182
- 183
- 184
- 185
- 186
- 187
- 188
- 189
- 190
- 191
- 192
- 193
- 194
- 195
- 196
- 197
- 198
- 199
- 200
- 201
- 202
- 203
- 204
- 205
- 206
- 207
- 208
- 209
- 210
- 211
- 212
- 213
- 214
- 215
- 216
- 217
- 218
- 219
- 220
- 221
- 222
- 223
- 224
- 225
- 226
- 227
- 228
- 229
- 230
- 231
- 232
- 233
- 234
- 235
- 236
- 237
- 238
- 239
- 240
- 241
- 242
- 243
- 244
- 245
- 246
- 247
- 248
- 249
- 250
- 251
- 252
- 253
- 254
- 255
- 256
- 257
- 258
- 259
- 260
- 261
- 262
- 263
- 264
- 265
- 266
- 267
- 268
- 269
- 270
- 271
- 272
- 273
- 274
- 275
- 276
- 277
- 278
- 279
- 280
- 281
- 282
- 283
- 284
- 285
- 286
- 287
- 288
- 289
- 290
- 291
- 292
- 293
- 294
- 295
- 296
- 297
- 298
- 299
- 300
- 301
- 302
- 303
- 304
- 305
- 306
- 307
- 308
- 309
- 310
- 311
- 312
- 313
- 314
- 315
- 316
- 317
- 318
- 319
- 320
- 321
- 322
- 323
- 324
- 325
- 326
- 327
- 328
- 329
- 330
- 331
- 332
- 333
- 334
- 335
- 336
- 337
- 338
- 339
- 340
- 341
- 342
- 343
- 344
- 345
- 346
- 347
- 348
- 349
- 350
- 351
- 352
- 353
- 354
- 355
- 356
- 357
- 358
- 359
- 360
- 361
- 362
- 363
- 364
- 365
- 366
- 367
- 368
- 369
- 370
- 371
- 372
- 373
- 374
- 375
- 376
- 377
- 378
- 379
- 380
- 381
- 382
- 383
- 384
- 385
- 386
- 387
- 388
- 389
- 390
- 391
- 392
- 393
- 394
- 395
- 396
- 397
- 398
- 399
- 400
- 401
- 402
- 403
- 404
- 405
- 406
- 407
- 408
- 409
- 410
- 411
- 412
- 413
- 414
- 415
- 416
- 417
- 418
- 419
- 420
- 421
- 422
- 423
- 424
- 425
- 426
- 427
- 428
- 429
- 430
- 431
- 432
- 433
- 434
- 435
- 436
- 437
- 438
- 439
- 440
- 441
- 442
- 443
- 444
- 445
- 446
- 447
- 448
- 449
- 450
- 451
- 452
- 453
- 454
- 455
- 456
- 457
- 458
- 459
- 460
- 461
- 462
- 463
- 464
- 465
- 466
- 467
- 468
- 469
- 470
- 471
- 472
- 473
- 474
- 475
- 476
- 477
- 478
- 479
- 480
- 481
- 482
- 483
- 484
- 485
- 486
- 487
- 488
- 489
- 490
- 491
- 492
- 493
- 494
- 495
- 496
- 497
- 498
- 499
- 500
- 501
- 502
- 503
- 504
- 505
- 506
- 507
- 508
- 509
- 510
- 511
- 512
- 513
- 514
- 515
- 516
- 517
- 518
- 519
- 520
- 521
- 522
- 523
- 524
- 525
- 526
- 527
- 528
- 529
- 530
- 531
- 532
- 533
- 534
- 535
- 536
- 537
- 538
- 539
- 540
- 541
- 542
- 543
- 544
- 545
- 546
- 547
- 548
- 549
- 550
- 551
- 552
- 553
- 554
- 555
- 556
- 557
- 558
- 559
- 560
- 561
- 562
- 563
- 564
- 565
- 566
- 567
- 568
- 569
- 570
- 571
- 572
- 573
- 574
- 575
- 576
- 577
- 578
- 579
- 580
- 581
- 582
- 583
- 584
- 585
- 586
- 587
- 588
- 589
- 590
- 591
- 592
- 593
- 594
- 595
- 596
- 597
- 598
- 599
- 600
- 601
- 602
- 603
- 604
- 605
- 606
- 607
- 608
- 609
- 610
- 611
- 612
- 613
- 614
- 615
- 616
- 617
- 618
- 619
- 620
- 621
- 622
- 623
- 624
- 625
- 626
- 627
- 628
- 629
- 630
- 631
- 632
- 633
- 634
- 635
- 636
- 637
- 638
- 639
- 640
- 641
- 642
- 643
- 644
- 645
- 646
- 647
- 648
- 649
- 650
- 651
- 652
- 653
- 654
- 655
- 656
- 657
- 658
- 659
- 660
- 661
- 662
- 663
- 664
- 665
- 666
- 667
- 668
- 669
- 670
- 671
- 672
- 673
- 674
- 675
- 676
- 677
- 678
- 679
- 680
- 681
- 682
- 683
- 684
- 685
- 686
- 687
- 688
- 689
- 690
- 691
- 692
- 693
- 694
- 695
- 696
- 697
- 698
- 699
- 700
- 701
- 702
- 703
- 704
- 705
- 706
- 707
- 708
- 709
- 710
- 711
- 712
- 713
- 714
- 715
- 716
- 717
- 718
- 719
- 720
- 721
- 722
- 723
- 724
- 725
- 726
- 727
- 728
- 729
- 730
- 731
- 732
- 733
- 734
- 735
- 736
- 737
- 738
- 739
- 740
- 741
- 742
- 743
- 744
- 745
- 746
- 747
- 748
- 749
- 750
- 751
- 752
- 753
- 754
- 755
- 756
- 757
- 758
- 759
- 760
- 761
- 762
- 763
- 764
- 765
- 766
- 767
- 768
- 769
- 770
- 771
- 772
- 773
- 774
- 775
- 776
- 777
- 778
- 779
- 780
- 781
- 782
- 783
- 784
- 785
- 786
- 787
- 788
- 789
- 790
- 791
- 792
- 793
- 794
- 795
- 796
- 797
- 798
- 799
- 800
- 801
- 802
- 803
- 804
- 805
- 806
- 807
- 808
- 809
- 810
- 811
- 812
- 813
- 814
- 815
- 816
- 817
- 818
- 819
- 820
- 821
- 822
- 823
- 824
- 825
- 826
- 827
- 828
- 829
- 830
- 831
- 832
- 833
- 834
- 835
- 836
- 837
- 838
- 839
- 840
- 841
- 842
- 843
- 844
- 845
- 846
- 847
- 848
- 849
- 850
- 851
- 852
- 853
- 854
- 855
- 856
- 857
- 858
- 859
- 860
- 861
- 862
- 863
- 864
- 865
- 866
- 867
- 868
- 869
- 870
- 871
- 872
- 873
- 874
- 875
- 876
- 877
- 878
- 879
- 880
- 881
- 882
- 883
- 884
- 885
- 886
- 887
- 888
- 889
- 890
- 891
- 892
- 893
- 894
- 895
- 896
- 897
- 898
- 899
- 900
- 901
- 902
- 903
- 904
- 905
- 906
- 907
- 908
- 909
- 910
- 911
- 912
- 913
- 914
- 915
- 916
- 917
- 918
- 919
- 920
- 921
- 922
- 923
- 924
- 925
- 926
- 927
- 928
- 929
- 930
- 931
- 932
- 933
- 934
- 935
- 936
- 937
- 938
- 939
- 940
- 941
- 942
- 943
- 944
- 945
- 946
- 947
- 948
- 949
- 950
- 951
- 952
- 953
- 954
- 955
- 956
- 957
- 958
- 959
- 960
- 961
- 962
- 963
- 964
- 965
- 966
- 967
- 968
- 969
- 970
- 971
- 972
- 973
- 974
- 975
- 976
- 977
- 978
- 979
- 980
- 981
- 982
- 983
- 984
- 985
- 986
- 987
- 988
- 989
- 990
- 991
- 992
- 993
- 994
- 995
- 996
- 997
- 998
- 999
- 1000

- Artist Picture button
- Artist Picture object
- Track List button
- Track List Information object
- Track List Selector object (click to play)
- Track Name object
- Track Credits button
- CD Name object
- CD Credits button
- CD Credits object
- Generic (Configurable) Metadata button
- Generic Metadata object and more.

- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28
- 29
- 30
- 31
- 32
- 33
- 34
- 35
- 36
- 37
- 38
- 39
- 40
- 41
- 42
- 43
- 44
- 45
- 46
- 47
- 48
- 49
- 50
- 51
- 52
- 53
- 54
- 55
- 56
- 57
- 58
- 59
- 60
- 61
- 62
- 63
- 64
- 65
- 66
- 67
- 68
- 69
- 70
- 71
- 72
- 73
- 74
- 75
- 76
- 77
- 78
- 79
- 80
- 81
- 82
- 83
- 84
- 85
- 86
- 87
- 88
- 89
- 90
- 91
- 92
- 93
- 94
- 95
- 96
- 97
- 98
- 99
- 100

- Artist URL button and more.

- Player Name object
- Player URL button
- Sample button
- Download button
- Purchase button
- Recent button

- Label/Provider/Store Advertisement object
- Label/Provider/Store URL button

- 3. Copy/Play Management Components 1504

- [0344] These components handle set up of encryption keys, Watermark processing, Copy management, and more. Interfaces also exist for communication with the Clearinghouse(s) 105, transmission of purchase requests, and more, for special services such as pay per listen or cases where such access to the Content 113 is accounted for. Currently, the communications to the Clearinghouse(s) 105 functions are handled by the SCA(s) Processor 102.

- [0345] The use of the Content 113 by the Player Application 105 or Content Provider(s) 101 can be logged into database such as the License Database 107. The tracking of each use of Content 113 by the Player Application 105 can be transmitted to one or more logging sites such as the Clearinghouse(s) 105 or Content Provider(s) 101. The transmission can be scheduled at predetermined times to upload the usage information to the logging site. One predetermined time traffic, the Player Application 105 using known techniques, wake-up at a scheduled time, and transmit the information from the local logging database to the logging site. By reviewing the logging information, the Content 113, such as different members of a family, the identification of the user of the Content 113 is transmitted along with the usage information to the logging site. In another embodiment, the instead of logging the usage of Content 113 for later uploading to a logging site, the use of the Content 113 is uploaded to a logging site during every use of the Content 113. For example, when duplicating or copying the Content 113 stored at the End User Device(s) 105, on an external device such as DVD Disc, digital tape, flash memory, mini Disc or equivalent removable media, the use is uploaded to the logging site such as the Content 113 during their playback. This ensures the actual usage measurement makes this system more factual driven over systems using sampling methods, such as a Nielsen Rating scheme for television, or telephone surveys, where only a limited number of users are sampled at any one time and the results extrapolated. In this embodiment, the actual usage is measured by the Player Application 105 and the results extrapolated onto a designated web site such as the Electronic Digital Content Store(s) 103 or Content Provider(s) 101.

- [0346] In addition, other information about the Content 113 can be uploaded to the logging site. For example, the last time (e.g., hour and day) the Content 113 was performed; how many times the Content 113 was performed; if the Content 113 has been duplicated or copied to an authorized external device such as DVD Disc, digital tape or mini Disc, in cases where there are multiple distinct users of a single Player Application 105 on the End User Device(s) 105, such as different members of a family, the identification of the user of the Content 113 is transmitted along with the usage information to the logging site. By reviewing the usage information uploaded to the logging site, the Content Provider(s) 101 can measure the popularity of the Content 113 based on the actual usage, the identification of the user and the number of times the Content 113 has been performed. The actual usage measurement makes this system more factual driven over systems using sampling methods, such as a Nielsen Rating scheme for television, or telephone surveys, where only a limited number of users are sampled at any one time and the results extrapolated. In this embodiment, the actual usage is measured by the Player Application 105 and the results extrapolated onto a designated web site such as the Content 113 during their playback.

- [0347] In addition, other information about the Content 113 can be measured by the Player Application 105 on the End User Device(s) 105. For example, the last time (e.g., hour and day) the Content 113 was performed; how many times the Content 113 was performed; if the Content 113 has been duplicated or copied to an authorized external device such as DVD Disc, digital tape or mini Disc, in cases where there are multiple distinct users of a single Player Application 105 on the End User Device(s) 105, such as different members of a family, the identification of the user of the Content 113 is transmitted along with the usage information to the logging site. By reviewing the usage information uploaded to the logging site, the Content Provider(s) 101 can measure the popularity of the Content 113 based on the actual usage, the identification of the user and the number of times the Content 113 has been performed. The actual usage measurement makes this system more factual driven over systems using sampling methods, such as a Nielsen Rating scheme for television, or telephone surveys, where only a limited number of users are sampled at any one time and the results extrapolated. In this embodiment, the actual usage is measured by the Player Application 105 and the results extrapolated onto a designated web site such as the Content 113 during their playback.

- [0348] These components use the keys acquired by the Copy/Play

6. Inter-application Communication Components 1608

[0350] These components are used for coordination between the Secure Digital Content Electronic Distribution Player and other applications (e.g., browser, helper-app and/or plug-in, etc) that may invoke the Player Application 195, or that the Player Application 195 needs to use when carrying out its functions. For example, when a URL is activated, it invokes the appropriate browser and instruct it to load the appropriate page.

7. Other Miscellaneous Components

[0351] Individual components that don't fall into the categories above (e.g., instantiation) are grouped here.

8. The Generic Player

[0352] In this section the combining of the components above into a version of the Player Application 195 is discussed. This is just one of many different examples possible, since the Player Application 195 is designed for customization by being based on software objects. The Player Object Manager 1501 is a generic framework holding all the other components together. As discussed in the sections below, the blocks below the Player Object Manager 1501 in this diagram are required for any player, but may be replaced by specialized versions depending on such things as form of encryption or scrambling being used, types of audio compression, access methods for the Content 113 library, and more.

[0353] Above the Player Object Manager 1501 are Variable Objects 1512, which are mostly derived from the media-data associated with the Content 113 being played or searched. These Variable Objects are made available to the End-User Device(s) 195 by way of the End-User Display 1510 and received input from the End-User Controls 1511. All objects are configurable, and the layouts of all containers are customizable. These objects may be implemented in C/C++, Java or any equivalent programming language.

Using the Player Application 195

[0354] The following embodiment is for an example where the Player Application 195 running on End-User Device 195 is an audio player where Content 113 is music. It should be understood to those skilled in the art that other types of Content 113 can be supported by the Player Application 195. A typical audio enthusiast has a library of CDs holding songs. All of these are available within the Secure Digital Content Electronic Distribution System 100. The set of songs that have been purchased from Electronic Digital Content Store(s) 103 are stored within a Digital Content Library 196 on his or her system. The groupings of songs that are analogous to physical CDs are stored as Playlists. In some cases a Play-list exactly emulates a CD (e.g., all tracks of a commercially available CD has been purchased from an Electronic Digital Content Store(s) 103 as an on-line version of the CD and is defined by a Play-list equivalent Content Library on their systems. However for the purpose of the ensuing discussions, an example of a custom made music CD is used when the term a Play-list is mentioned.

[0355] When the End-User(s) 195 starts the Player Application 195 explicitly, rather than having it start up via invocation from the SDC(s) Processor 102, Application 195 proceeds to the last Play-list that was a selected. If no Play-lists exist in the Digital Content Library 196, the Play-list editor is started automatically (unless the user has turned off this feature via a preference setting). See **The Play-list** below for further details.

[0356] The Player Application 195 may also be invoked with a specific song as an argument, in which case it immediately enters Song-Play mode. Optionally, the song may be prepared for play but await action by the End-User(s) before proceeding. See **Song Play** below for more on this situation.

[0357] The Play-list (corresponding screen of an End-User Interface 1603):

- [0357] When the End-User(s) 195 has invoked the Play-list function, these are the available functions:
 - **Open Play-list**
 - **Digital Content Librarian** is invoked to display a list of stored Play-lists for selection. Also see **Digital Content Librarian** below for more info.
 - **Edit Play-list**
 - Invokes the Play-list Editor (see below), primed with the current Play-list if one has been loaded already. Otherwise the editor creates an empty Play-list to start with.
 - **Run Play-list**
 - Songs are played one at a time starting with the selected song (or the beginning of the play-list, if no song is selected). Options set in the Play-list Editor affect the sequencing of the playback. However there is control avail-

able here to override those options for this play of the Play-list.

- **Play song**
- Only the selected song from the Play-list is played. See **Song Play** below for more info.
- **Play-list info**
- Display information about the Play-list.
- **Song info**
- Display information about the selected song within the Play-list.
- **Visit web site**
- Visit web site associated with this Play-list from browser.

[0359] Open the Digital Content Librarian window. Also see **Digital Content Librarian** below for more info.

- **[0360] The Play-list Editor** (corresponding screen of an End-User Interface 1603):
- **View/Create/Delete Play-list**
- When invoking the Play-list editor, these are the End-User(s) 195 options:
 - View/Load/Delete Play-list
 - see **Digital Content Librarian** below for more info.
 - Save Play-list
- **Current version of Play-list is saved in the Digital Content Library 198.**
- **Delete Song**
- Currently selected song is deleted from Play-list.
- **Add Song**
- **Digital Content Librarian** is invoked in song-search mode, for selection of song to add to the Play-list. Also see **Digital Content Librarian** below for more info.

[0360] When the Play-list Editor is invoked, the Play-list is displayed. The Play-list is a list of stored Play-lists for selection of one to load or delete. Also see **Digital Content Librarian** below for more info.

- **[0361] When the Play-list is loaded, the following options are available:**
- **View/Load/Delete Play-list**
- **End-User(s) notes about the song**
- **Lead-In delay on playing the song**
- **Follow-on delay after playing the song**
- **Start-point within song when playing**
- **End-point within song when playing**
- **Weighting for random mode**
- **Volume adjustment for this song and more.**

[0361] Set Play-list attributes: Display and allow changes to the attributes of this Play-list. These attributes may be set:

- **Play-list title**
- **Play-list mode (random, sequential, etc)**
- **Repeat mode (play once, restart when done, etc)**
- **End-User(s) notes about this Play-list**

[0362] Librarian (corresponding screen of an End-User Interface 1601):

- Open the Digital Content Librarian window. Also see **Digital Content Librarian** below for more info.

[0363] When a song has been prepared for play, either by invoking the Player Application 195 with the song as an argument or by selecting a song for play from Play-list or within the Digital Content Librarian, these are the End-User(s) options: (corresponding screen of an End-User Interface 1601):

- **Play**
- **Pause**
- **Stop**

4 *• Skip Backward*
• Skip Forward
• Adjust Volume
• Adjust Track Position

5 *• View Lyrics*
• View Credits
• View CD Cover
• View Artist Picture
• View Track Information
• View other metadata
• Visit web site
• Playlist
• Librarian and more.

6 **[0364] Digital Content Librarian** The Digital Content Librarian can be invoked implicitly when selecting songs or playlists (see above) or may be opened in its own window for management of the Song Library on the End-User(s)' system. In that case, these are the End-User(s) options:

7 **Working with songs:**

8 *Sort All by Artist, Category, Label, other*
Select Songs by Artist, Category, Label, other
Add Selected songs to Current Playlist
Copy Song to CD (if enabled)
Delete Song
Add Song to Category and more.

9 **Work with Playlist:**

10 *Sort by Name*
Sort by Category
Search by Keyword
Search by Included Song Title
Load Selected Playlist
Remove Playlist
Create CD from Selected Playlist (if enabled) and more.

11 **[0365] Turning now to FIG. 18 is a flow diagram of a process running on End-User Device 9 for tracking content** individually, according to the present invention. A Content ID 1802 is provided by the Content Provider 101 during content preparation. In one embodiment, the Content ID 1802 is part of the Content SCI(s) 630 during the content creation process with Secure Container Packer Tool 182. In another embodiment, the Content ID 1802 is part of the Meta data SCI(s) 620 (containing promotional data). The Content ID 1802 is an identifier that is unique to the content being processed.

12 **[0366] A Transaction ID 538 is part of the Transaction Data 642 along with the Content ID 1802. In the Transaction** SCI(s) 640 built by the Transaction Processor Module 175 as discussed previously. The Transaction ID 633 is a unique identifier for each over all purchase transaction from an End User Device(s) 109. In addition, an Item Number 1806 is a unique identifier generated by the Electronic Digital Content Store 103 for each for each place or member or title that forms part of the transaction. Stated Item Number 1806 tracks each item purchased under the Transaction ID 535.

13 **[0367] Focusing now to the operation on the End User Device 9 is received** by the End User Device 109. In addition, an Offer SCI(s) with the content ID 1802 also contained within Transaction ID 535 is received. A Purchase ID 1808 is created on the End User Device 109. In one embodiment, the Purchase ID 1808 is a concatenation operation 1810 of three numbers, specifically, the Content ID 1802 with the Transaction ID 535 with the Item Number 1806. It should be understood that other types of combinations aside concatenation operation 1810 could be used to generate the Purchase ID 1808 such as hashing all three numbers together or other mathematical combinations that result in a unique Purchase ID 1808. The process of combining the three numbers can be done in using the Tamper Resistant Code technology previously discussed above in the Player Application to prevent unauthorized access to the Purchase

14 **[0368] Once a unique Purchase ID 1812 is created and associated for each piece of Content 113, the Player Application 195 on End User Device 109 can track store usage conditions 519 for each piece of Content 113, even if there is more than one copy of the identical Content 113 such as a song, stored on End User Device 109.**

15 **Claims**

16 **1. A method for uniquely identifying digital content on an digital content player comprising the steps of:**

17 **receiving a first identifier which uniquely identifies the content received from a content provider;**
receiving a second identifier which uniquely identifies a transaction by which the content was received;
receiving a third identifier which uniquely identifies the item in a transaction by which the content was received;
and
producing a fourth unique identifier based upon the mathematical combination of the first identifier, the second identifier, the third identifier, and the third identifier;

18 **2. A method as claimed in claim 1, wherein the step of producing includes producing a fourth unique identifier based upon the concatenation of the first identifier, the second identifier and the third identifier;**

19 **3. A method as claimed in claim 1, wherein the step of receiving a second identifier includes receiving a unique identifier from a store which sells the content.**

20 **4. A method as claimed in claim 3, wherein the step of receiving a third identifier includes receiving a unique identifier from a store which sells the content, uniquely identifies a transaction by which the content was received.**

21 **5. A method as claimed in claim 1, further comprising the steps of:**

22 **associating the forth unique identifier with the content including any usage conditions; and**
reviewing the forth unique identifier with the content prior to playing the content.

23 **6. A method according to claim 1, wherein the step of producing a fourth unique identifier includes producing a forth unique identifier in a tamper resistant environment to prevent unauthorized access thereto.**

24 **7. A system for tracking usage of digital content on user devices, said system comprising:**

25 **a plurality of content sites for distributing digital content over computer readable medium to users, wherein** the content contains a unique content identifier associated therewith;

26 **a plurality of electronic stores for granting licenses to play digital content data to users, each electronic store** being coupled to a network, wherein the licenses contain a unique transaction identifier for uniquely identifying the transaction, and the licenses contain a unique item identifier for uniquely identifying at least one item in the transaction; and

27 **a plurality of content players for playing content data, each digital content player receiving from the network** a plurality of content players for playing content data, each digital content player receiving from the network the digital content data licensed by one of the users, wherein the content players produce a purchase identifier based upon the mathematical combination of the content identifier, the transaction identifier and the item identifier.

28 **8. A system for tracking usage of digital content on user devices as claimed in 7, wherein the mathematical combi-**nation is a concatenation.

29 **9. A system for tracking usage of digital content on user devices as claimed in claim 7, wherein the content player** comprises a tamper resistant environment and the purchase identifier is produced in the tamper resistant environment to prevent unauthorized accessed thereto.

30 **10. A digital content player for uniquely identifying digital content, comprising:**

31 **means for receiving a first identifier which uniquely identifies the content received from a content provider;**
means for receiving a second identifier which uniquely identifies a transaction by which the content was re-

6
 Content;
 means for receiving a third identifier which uniquely identifies the item in a transaction by which the content
 was received; and
 means for producing a fourth unique identifier based upon the mathematical combination of the first identifier,
 the second identifier, and the third identifier.

10
 11. A digital content player for uniquely identifying digital content as claimed in claim 10, wherein the means for pro-
 ducing includes producing a forth unique identifier based upon the concatenation of the first identifier, the second
 identifier and the third identifier.

12. A digital content player for uniquely identifying digital content as claimed in claim 10, wherein the means for re-
 ceiving a second identifier includes receiving a unique identifier from a store which sells the content.

13. The digital content player for uniquely identifying digital content as claimed in claim 10, wherein the means for
 receiving a third identifier includes receiving a unique identifier from a store which uniquely identifies a transaction
 by which was received.

14. A digital content player for uniquely identifying digital content as claimed in claim 10, further comprising:
 means for associating the fourth unique identifier with the content including any usage conditions and
 means for reviewing the usage conditions by indexing the fourth unique prior to playing the content.

15. A computer readable medium containing program instructions for uniquely identifying digital content on an digital
 content player tracking comprising the steps of any one of claim 1 to claim 6.

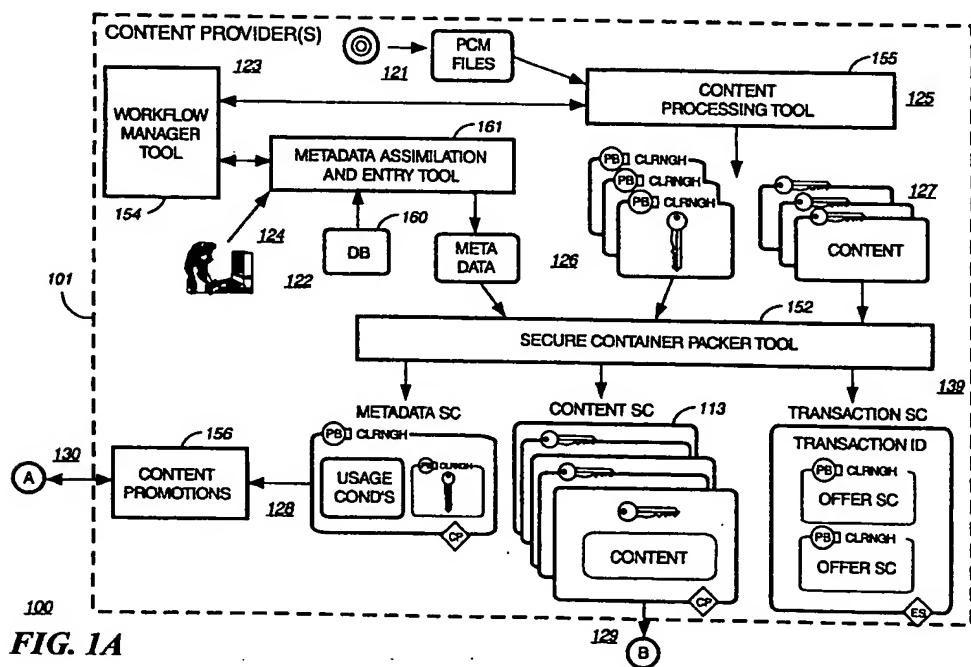
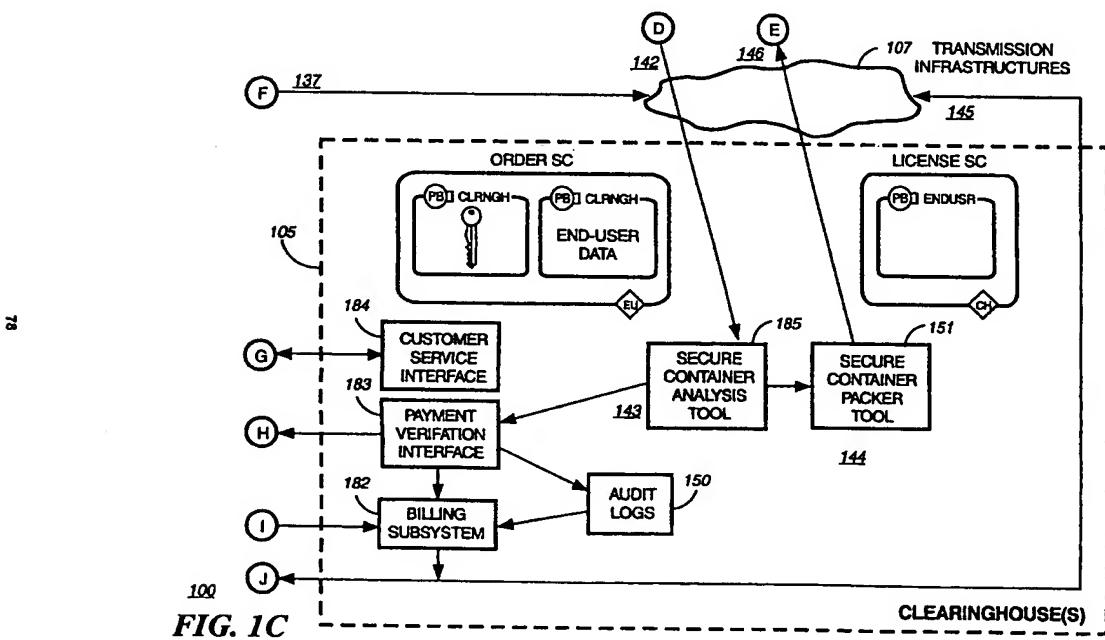
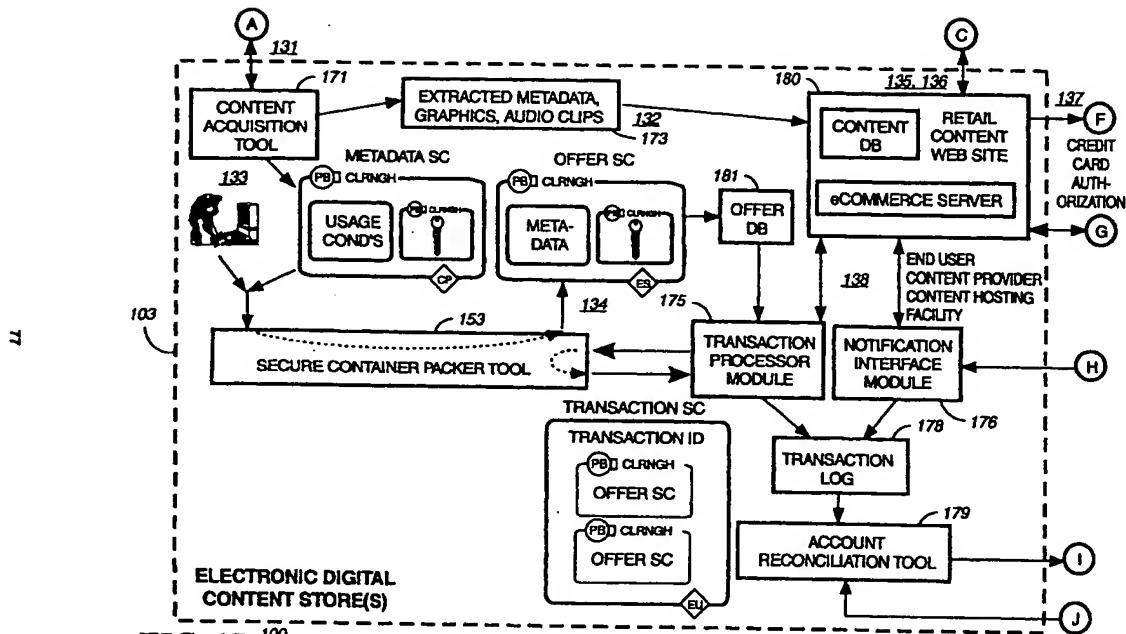
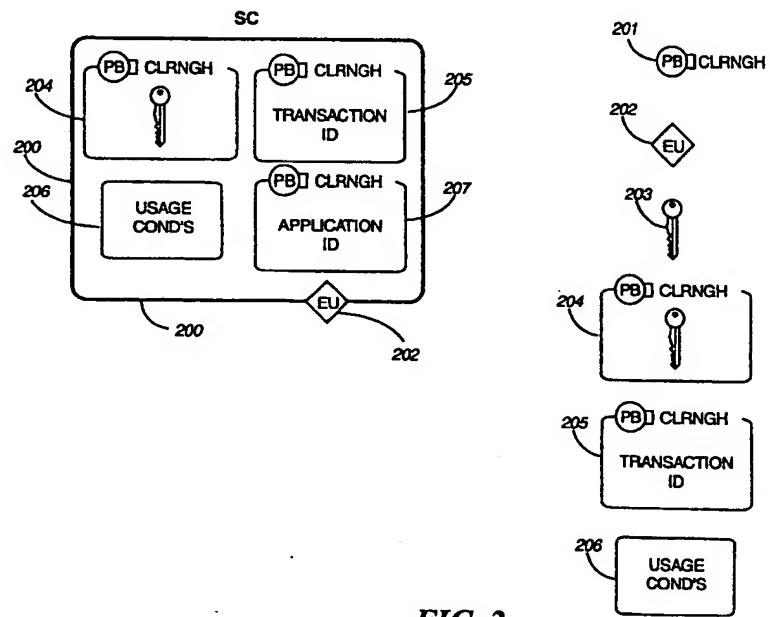
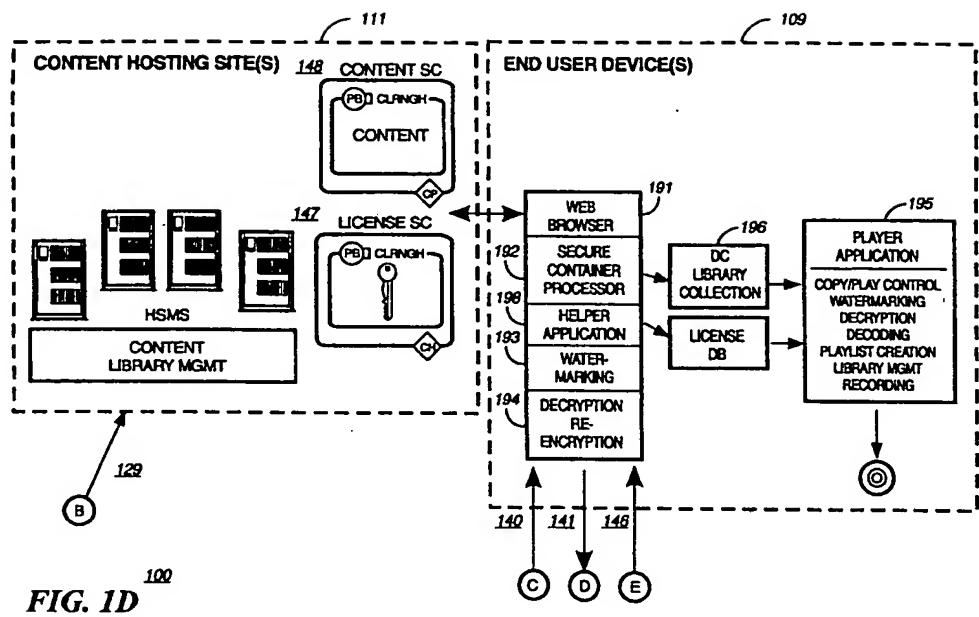


FIG. 1A





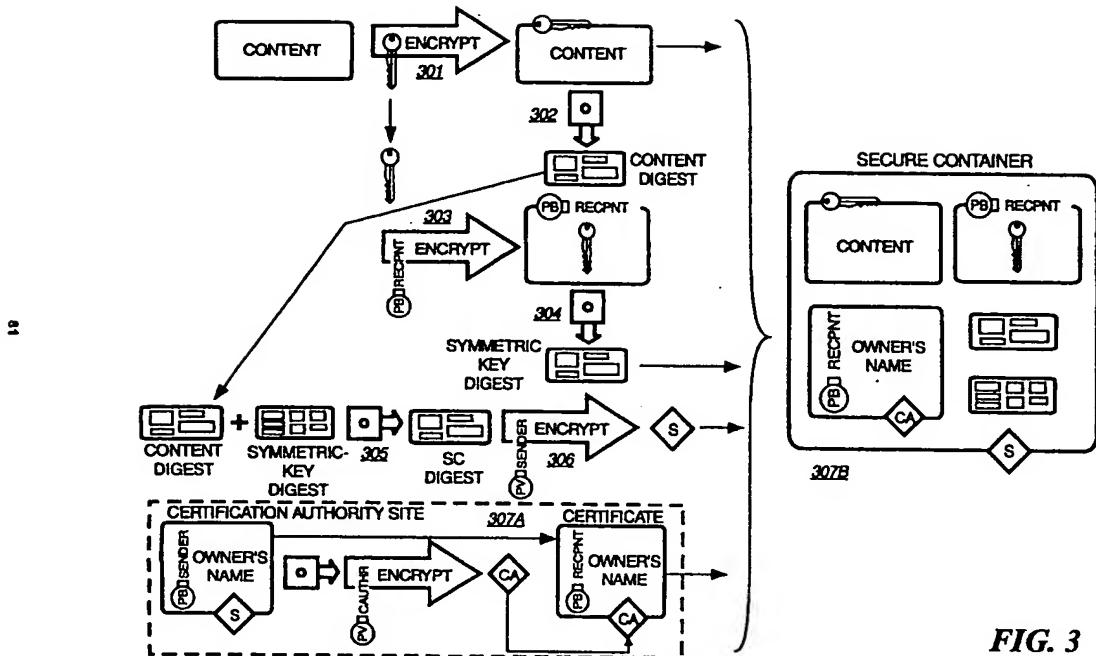


FIG. 3

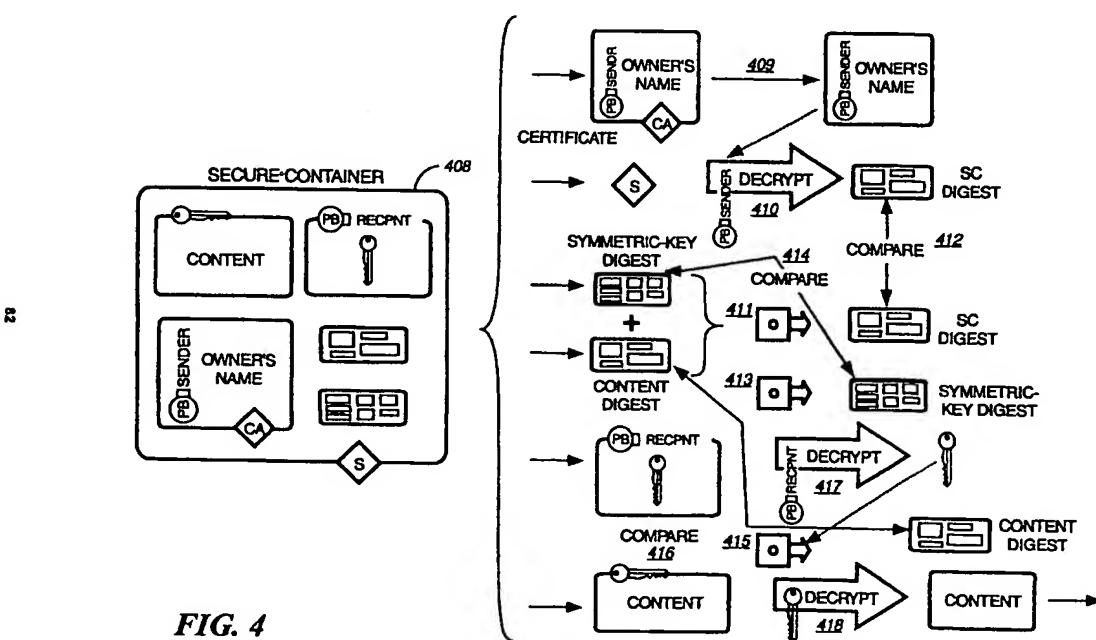


FIG. 4

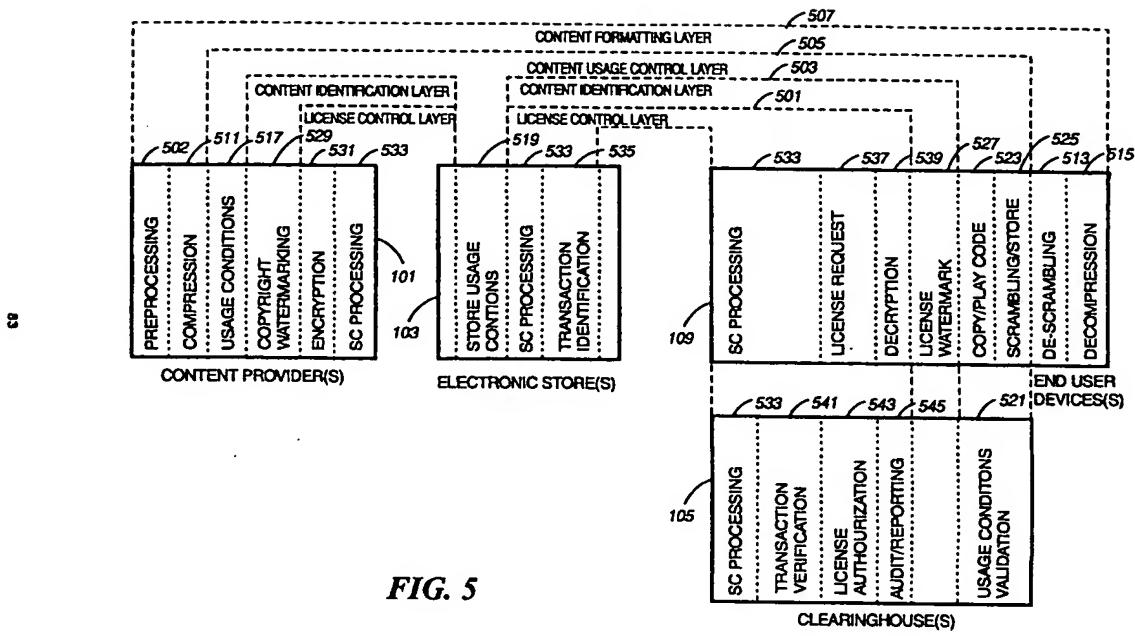


FIG. 5

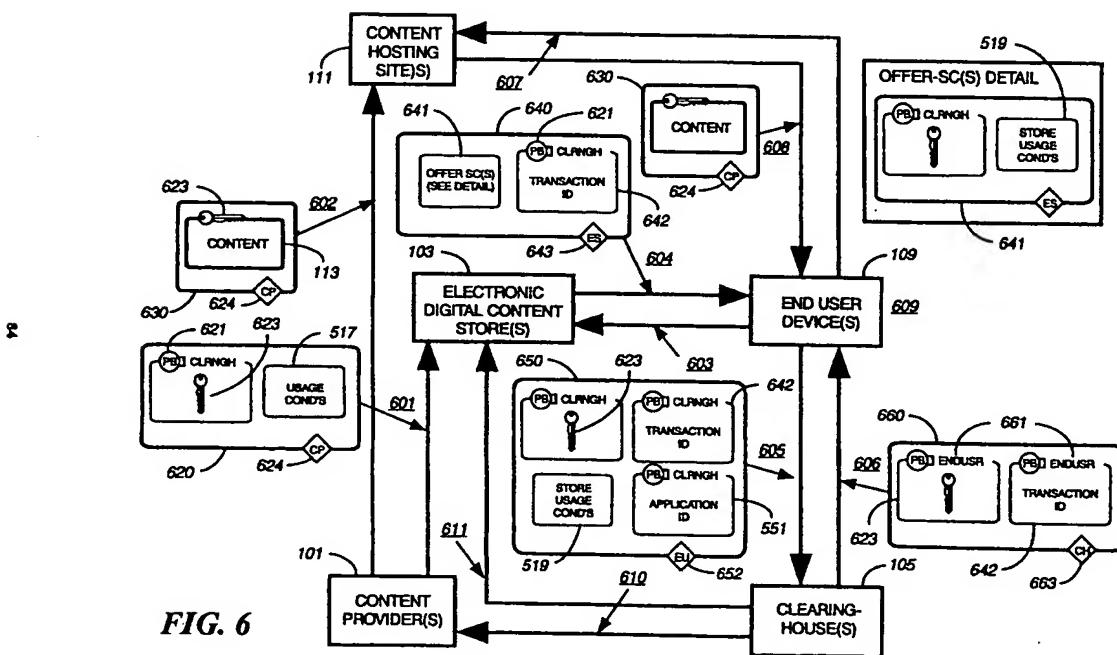


FIG. 6

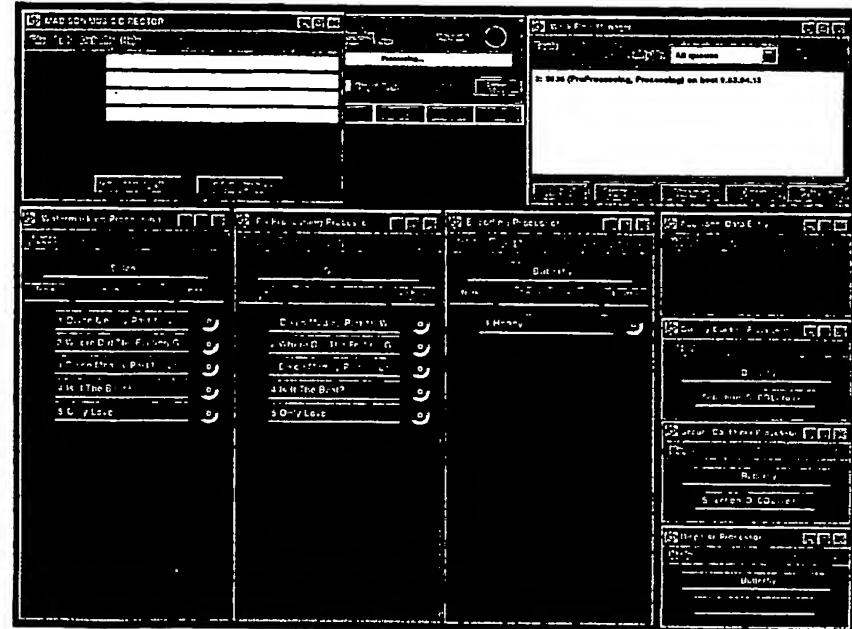


FIG. 7

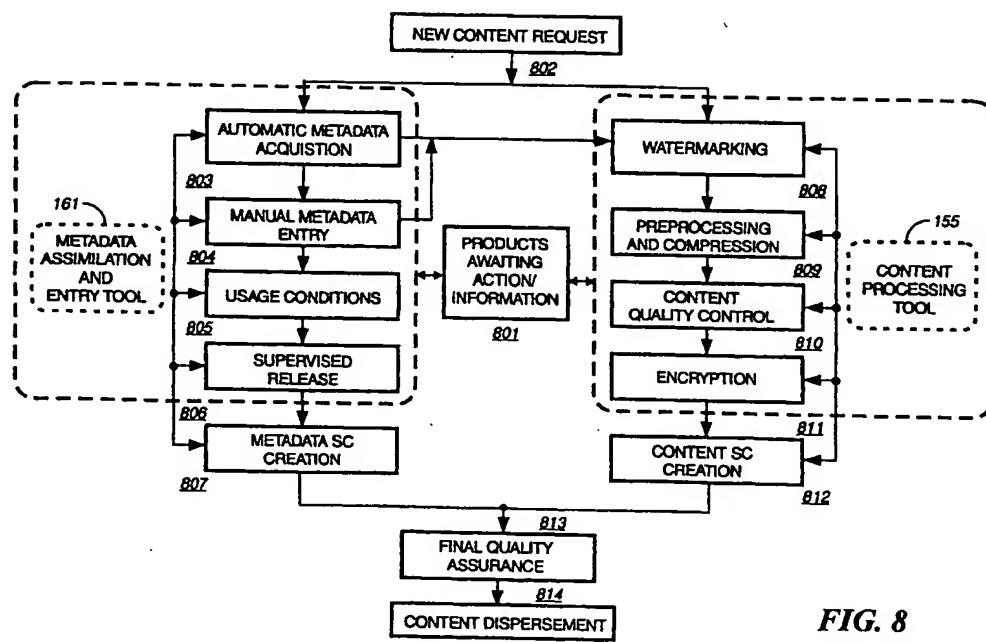


FIG. 8

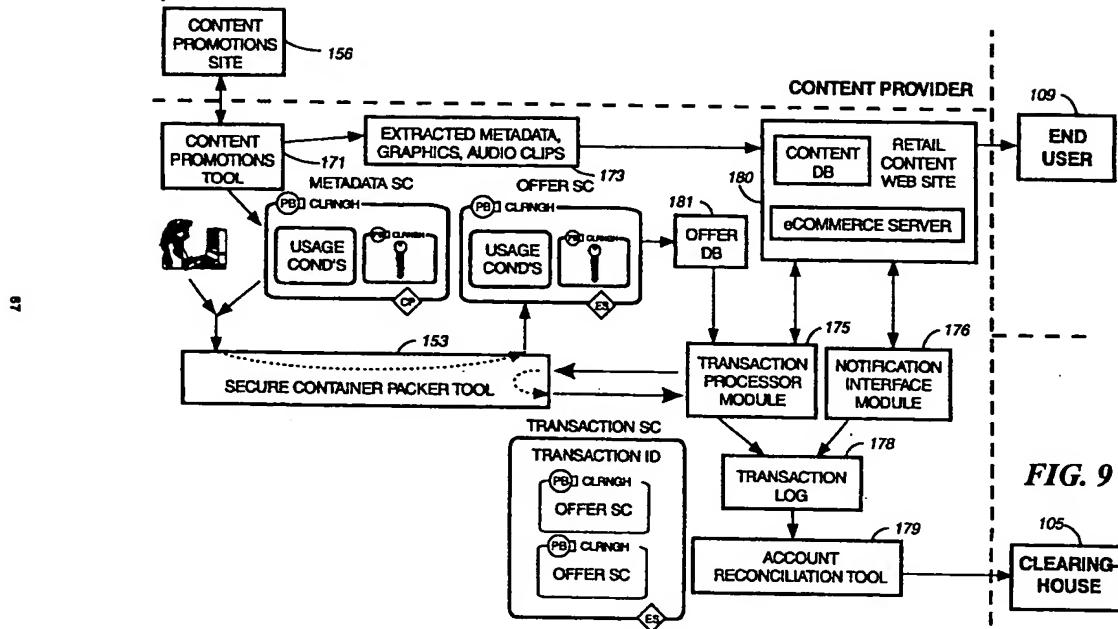


FIG. 9

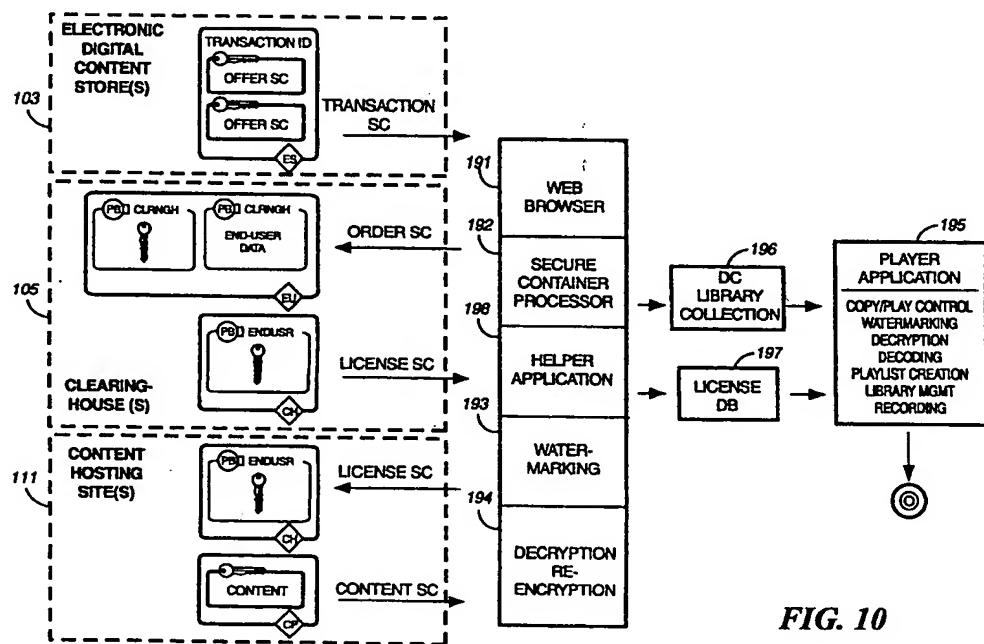


FIG. 10

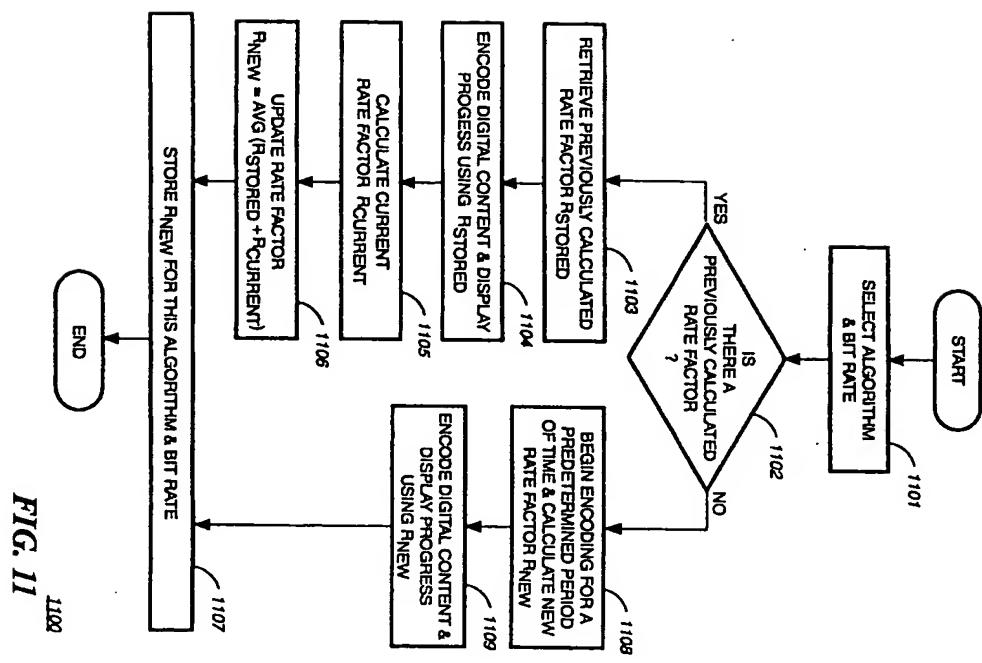
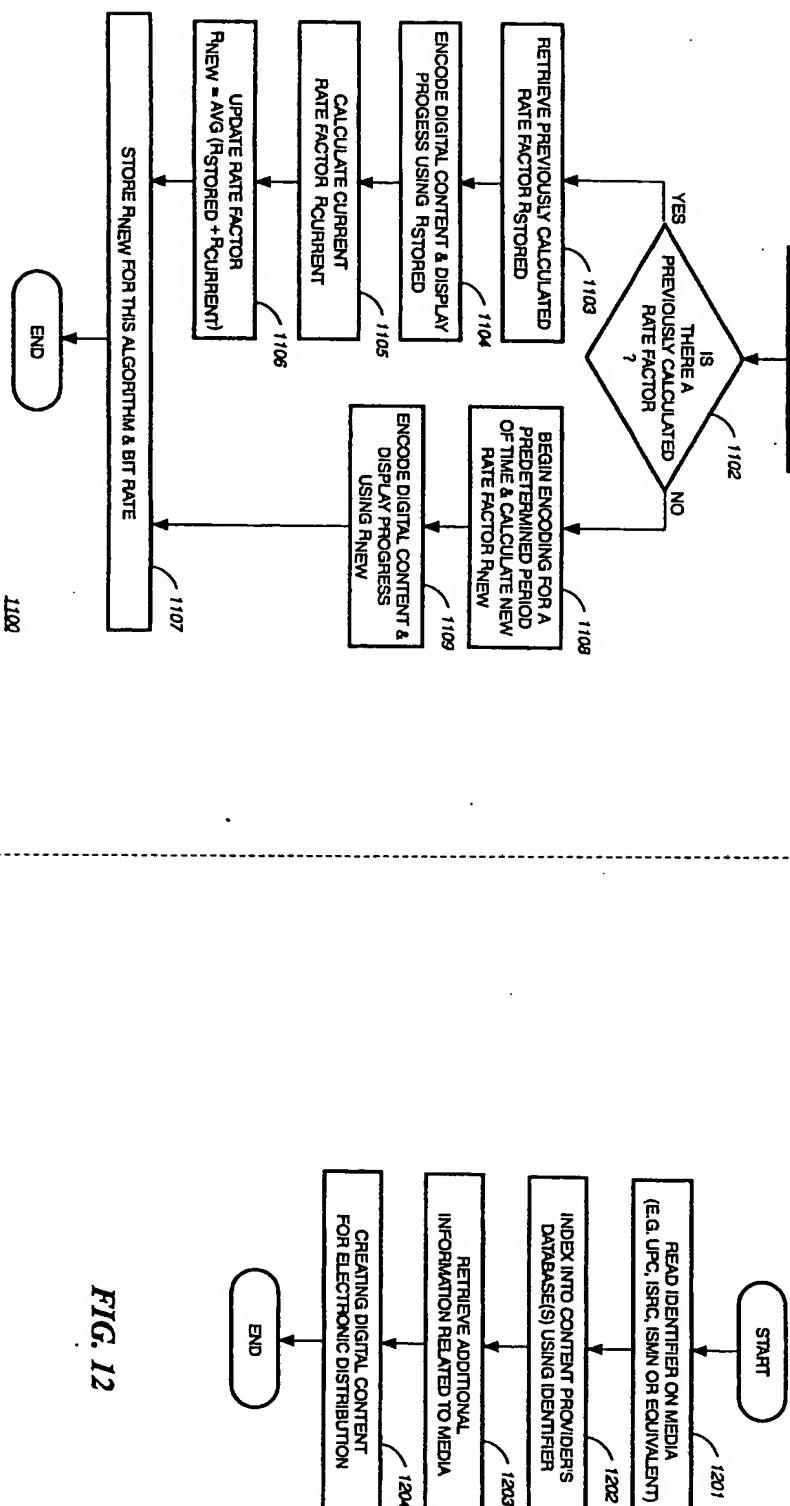


FIG. 11

89

FIG. 12



90

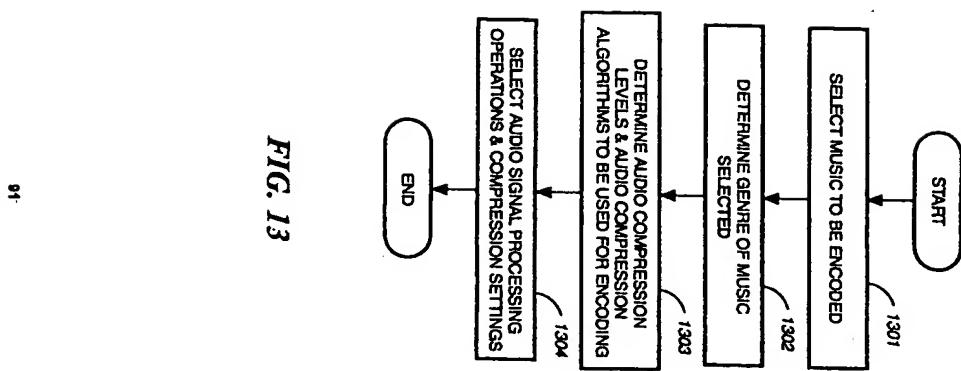


FIG. 13

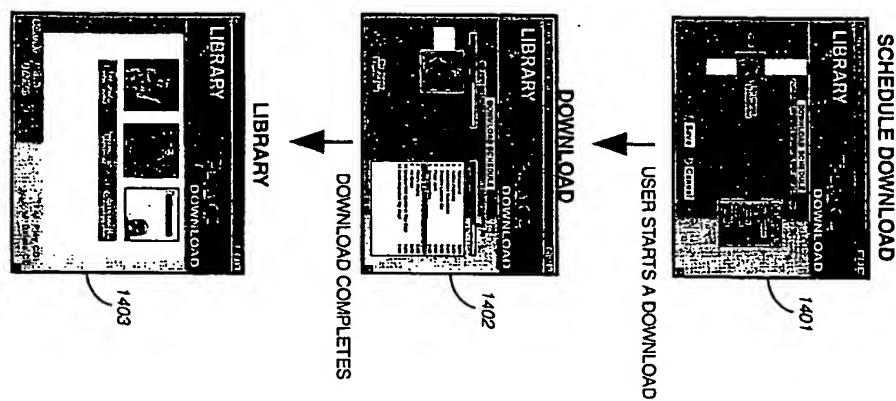


FIG. 14

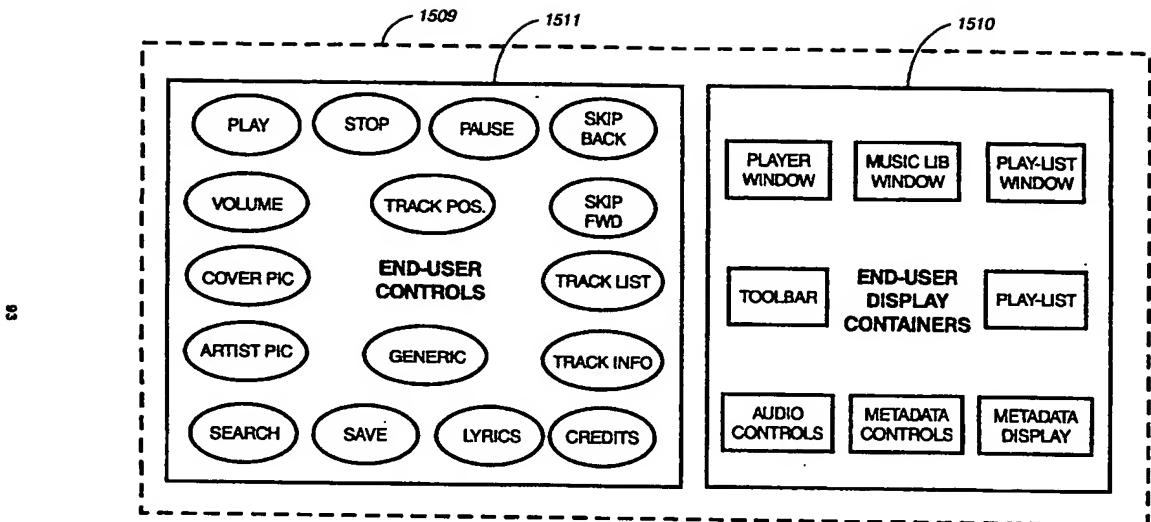


FIG. 15A

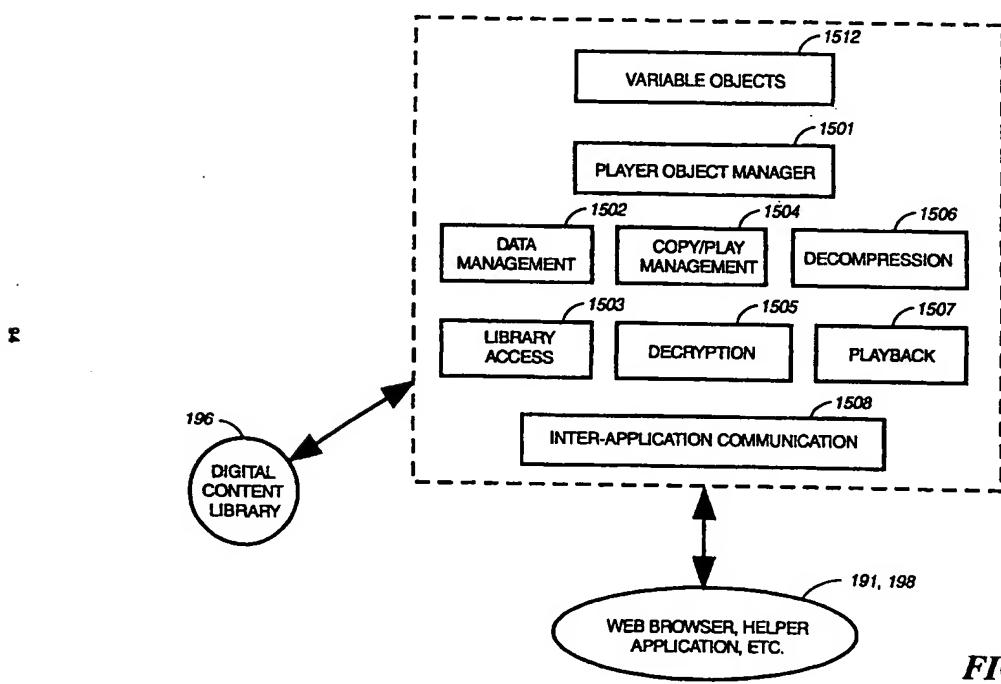
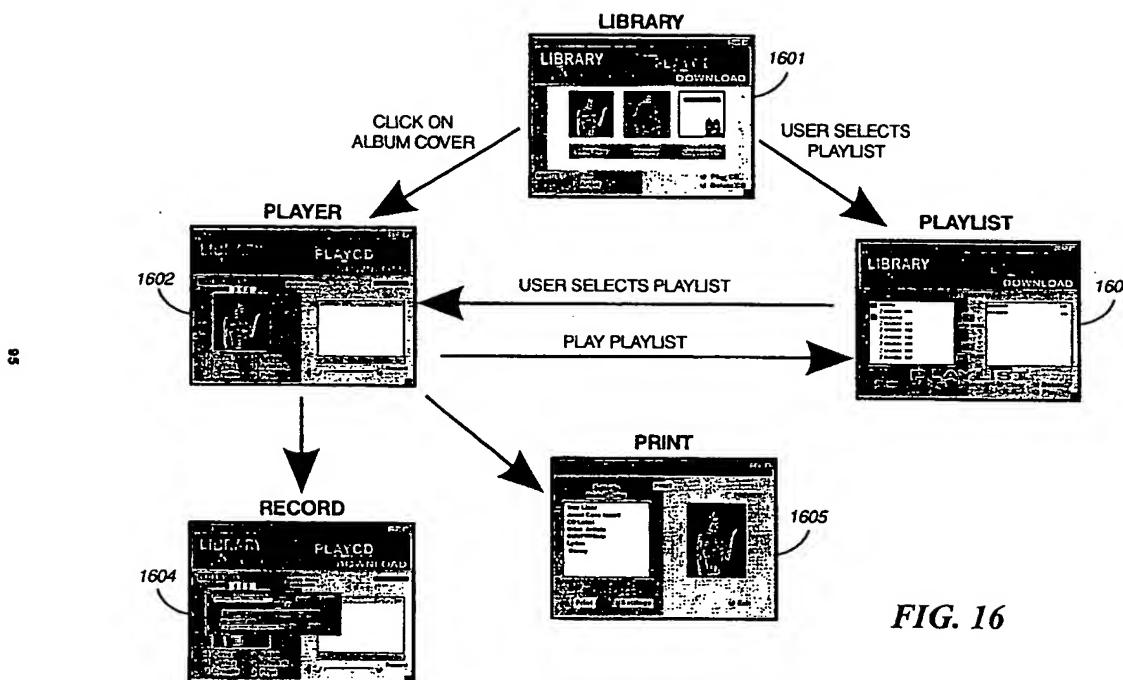
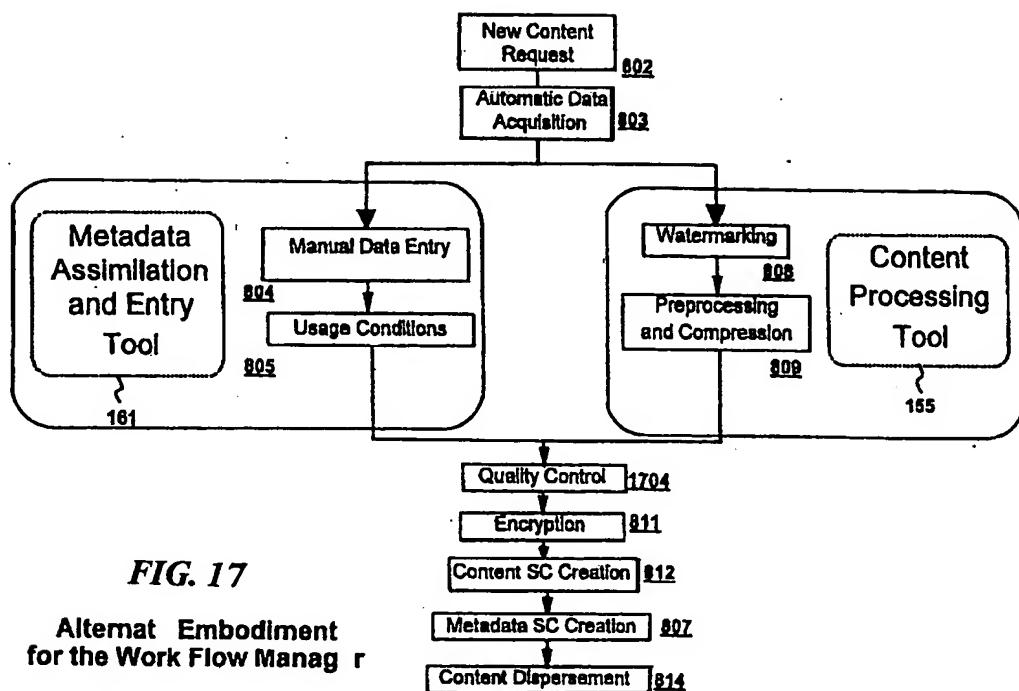


FIG. 15B



96

EP 1 085 443 A2



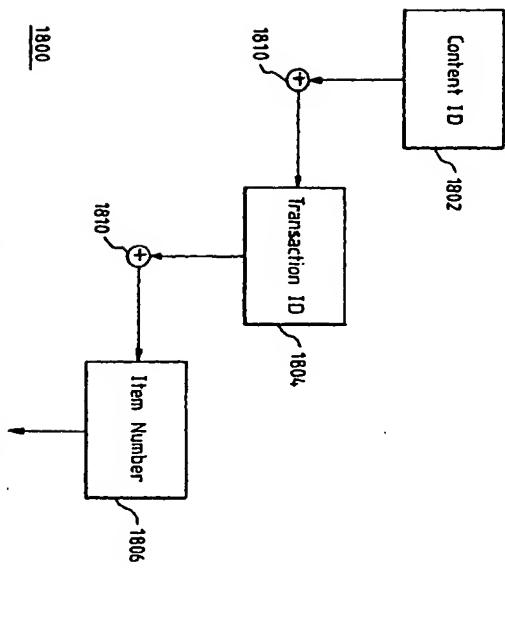


FIG. 18

